

number theory and its application to cryptography



Indulata Sukla

NUMBER THEORY AND ITS APPLICATION TO CRYPTOGRAPHY

INDULATA SUKLA
PROFESSOR OF MATHEMATICS,
SAMBALPUR UNIVERSITY
SAMBALPUR



KALYANI PUBLISHERS

LUDHIANA * NEW DELHI * NOIDA (U.P.)
HYDERABAD * CHENNAI * KOLKATA * CUTTACK

KALYANI PUBLISHERS

Head Office

B-I/292, Rajinder Nagar, Ludhiana-141 008

Administration Office

4779/23, Ansari Road

Daryaganj, **NEW DELHI-110 002**

Works :

B-16, Sector 8, **NOIDA (U.P.)**

Branch Offices :

1, Mahalakshmi Street,

T. Nagar, **CHENNAI-600 017**

110/111, Bharatia Towers, Badambadi

CUTTACK- (Orissa)

3-5-1108, Narayanaguda,

HYDERABAD-500 029

10/2B, Ramanath Mazumdar Street,

KOLKATA-700 009

1057 03 04 05

© 2004, Sukla Indulata

TYPESETTING AT

Gautam Graphic Printers, Mai Hiran Gate,

ISBN 81-272-1249-0

PRINTED IN INDIA

At Gayatri Offset Press, A-66, Sector 2, NOIDA

and published by Mrs. Usha Raj Kumar for

Kalyani Publishers, New Delhi-110 002

PREFACE

***In the sacred memory
of
my late parents***

***Kashinath Kar Mohapatra
and
Swarna Mayee Devi***

PREFACE

The present book is evolved from a course on analytic number theory offered at the Mathematics department of Sambalpur University during the last 25 years. It provides the basic knowledge of number theory and its application to cryptography suitable for one semester course in the Post Graduate level and also serves as a reference book for the teachers and for the beginners in number theory. The topics chosen and illustrated in this book are intended to provide some depth in the subject. Many problems of much interest are discussed together with some more exercises left for the students. The computer programming in BASIC are given at some places which will help students to work out in the computer for practice. In some cases algorithms are also described.

The goal of this work is to attract students to opt for the subject and do some fruitful researches in this field. Many of the students who have taken this course during the past 25 years have become professional teachers and contributed to number theory.

Apart from my students who have taken keen interest in my lectures, my sons Chuni and Lulu have always encouraged me in writing this book.

Lastly I acknowledge the authority of Sambalpur university for sanctioning me sabbatical leave to write this book.

Makara Sankranti, 2004

INDULATA SUKLA

CONTENTS

Chapters	Pages
0. INTRODUCTION	i—v
1. PRIME NUMBERS AND DISTRIBUTION OF PRIME NUMBER	1—47
1.1 Prime numbers	
1.2 Greatest Common divisor	
1.3 How many prime numbers are there?	
1.4 Twin primes	
1.5 Conjecture of Goldbach	
1.6 Fermat numbers	
1.7 Prime number of the form $n^n + 1, n^{n^n} + 1$ etc.	
1.8 Mersenne numbers	
1.9 Solution of equation in prime number	
1.10 Magic squares formed from prime number	
1.11 Distribution of prime numbers	
1.12 Some more numbers and their computer programming.	
Exercises	
2. ARITHMETICAL FUNCTIONS	48—74
2.1 Mobius function	
2.2 Euler's Totient function	
2.3 Arithmetical functions $d(n)$ and $\sigma(n)$	
2.4 Generalized Euler's Totient function	
2.5 Liouville's function	
2.6 Von-Mangoldt function	
2.7 Average arithmetic functions	
2.8 Computer programming for determining factorization of N , values of PHIN, TAUN and SIGMAN	
Exercises.	

3. CONGRUENCES

75—105

- 3.1 Definition and basic properties of congruences
- 3.2 Residue classes and complete residue systems
- 3.3 Reduced residue systems and the Eulers-Fermat theorems
- 3.4 Linear congruences.
- 3.5 Polynomial congruences modulo p , Lagrange's theorem
- 3.6 Application of Lagrange's theorem
- 3.7 Simultaneous linear congruences, the chinese remainder theorem and its application.
- 3.8 Some algorithms
Exercises

4. SOME THEOREMS ON DISTRIBUTION OF PRIME NUMBERS.

106—123

- 4.1 Introduction
- 4.2 Chebyshev's function $\psi(x)$ and $\theta(x)$
- 4.3 Some equivalent forms of the prime numbers theorem.
- 4.4 Inequalities for $p(n)$ and p_n .
- 4.5 The partial sums of Mobius function
Exercise

5. CRYPTOGRAPHY

124—133

- 5.1 Classical cryptosystem
- 5.2 Public-key cryptography
- 5.3 The RSA system
Exercises

6. PRIMITIVE ROOTS AND INDICES

134—150

- 6.1 Primitive Roots
- 6.2 Reduced residue system
- 6.3 Primitive roots modulo prime
- 6.4 The existence of primitive root modulo p^k
- 6.5 The existence of primitive root modulo $2p^k$
- 6.7 Application of Indices in solving congruences.
- 6.8 The discrete logarithm
Exercises

7. QUADRATIC RESIDUES AND QUADRATIC RECIPROCITY LAWS

151—177

- 7.1 Quadratic residues

- 7.2 Legendre's symbols and its properties
- 7.3 Gauss lemma
- 7.4 Quadratic reciprocity law and its application
- 7.5 The Jacobi symbol
- 7.6 Computing square root modulo p .
- 7.7 Application to cryptogarchy
- Exercises

8. PRIMALITY TESTING AND FACTORING 178—195

- 8.1 Pseudoprimes and Carmichael numbers
- 8.2 Strong pseudoprimes and probabilistic primality testing
- 8.3 Primality testing (Application of Primitive roots and indices to cryptography)
- 8.4 Pollard's $(p-1)$ method
- 8.5 Pollard's rho - method
- 8.6 Fermat's factorization method
- Exercises

ANSWER TO EXERCISES 196—197

APPENDIX 198—202

BIBLIOGRAPHY 203—204

INDEX 205—208

INTRODUCTION

The theory of numbers is that branch of mathematics which deals with properties of whole numbers, 1, 2, 3, 4, 5.... that is positive integers. Numbers, specially positive integers were used for keeping records and for commercial transaction for over 5000 years before any one thought of studying numbers in a systematic way. Many branches of mathematics have their origin in number theory. the first scientific approach to the study of integers that, the true origin of the theory of numbers, is generally attributed to the Greeks. Around 600 BC Pythagoras and his disciple made rather thorough studies of integers. They classified them to four categories even integers, odd integers, prime numbers and composite numbers.

A prime number is a number greater than 1 whose only divisors are 1 and the number itself. Numbers which are not prime are called as composite number. But the number 1 is neither a prime nor a composite number.

Pythagoreans also linked numbers with geometry. When the numbers are represented by dots arranged in the form of triangles, squares, pentagons, hexagons, septagons, octagons etc. they are called as triangular numbers, square numbers, pentagonal numbers, septagonal number, octagonal numbers respectively. In general if a number is represented by dots arranged in form of a polygon then the number is called polygonal number. These numbers specially triangular numbers and pentagonal numbers have importance in the study of partition theory.

Around 300 BC Euclid's *Elements* a collection of 13 books appeared. Three of these 13 books were devoted to the theory of numbers. (BOOK VI, IX and X). Euclid was the first mathematician to prove that there are infinite number of primes. There are also proofs of this theorem by other eminent mathematicians. There is also topological proof of this famous Euclid's theorem. Also we note that some primes are represented by the numbers of the form $4k \pm 1$, $6k \pm 5$, $8k \pm 3$, $8k \pm 1$, $k = 1, 2, 3, \dots$. Like Euclid's theorem, we have theorems which

The prime number theorem tells that

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

This conjecture was made independently by Gauss and Legendre. They attempted to prove this statement but failed. Later on in 1851 the Russian mathematician Chebyshev gave equivalent theorems of this statement.

Besides prime numbers there are other numbers in the world of numbers which have interesting properties. They are amicable numbers, Armstrong numbers and Fibonacci numbers.

Two integers m and n are said to be amicable or friendly numbers if the sum of the proper divisors of m is the number n and vice versa. The smallest amicable number pair is 220 and 284 because the divisors of 220 are 1, 2, 34, 5, 10, 11, 20, 22, 44, 55, 110 when added equals to 284 and again the divisors of 284 are 1, 2, 4, 71, 142, when added gives 220. There are other amicable pairs also. If the sum of the divisors of an integer n is less than $2n$, then it is called as 'deficient number'. On the other hand if the sum of the divisors of integer n is greater than $2n$, then n is called as abundant number. A sequence of integers u_1, u_2, \dots, u_n , is called Fibonacci sequence if $u_1 = 1, u_2 = 1, u_{n+1} = u_n + u_{n-1}$.

There are many interesting properties of Fibonacci numbers.. It is applied in Golden ratio.

The most emerging field of modern time is the Cryptography, the science of making communication unintelligible to all except authorized parties. Cryptography is the only known practical means for protecting information transmitted through public communication net works. It is a subject of common interest to both mathematician and computer scientists. Number theory has application to Cryptography. In 1977, R. Rivest, A. Shamir, and L. Adleman proposed a public key cryptosystem which uses only elementary ideas from number theory. Their system is popularly known as RSA after the initials of the inventors. Its security depends on the assumption that the factorization of composite numbers with large prime factors is time taking even in the computer. In this system each user chooses a pair of distinct primes, p and q , so large that the factorization of their product $n = pq$, is beyond all computational capabilities. After selecting n , the user chooses a random positive integer k , and the pair (n, k) is publicly known. Because the factors p and q are not known easily it is not possible for out siders party to decipher the message thus the security is maintained. Also it is not possible to say whether a given large number n is a prime or composite. It has to go through different primality tests. If n is not prime but composite there are methods due to Fermat and others to find factors

of the large number n . There are other different methods for the primality testing. It is interesting to study these methods.

Another application of congruential arithmetic is a public-key encryption method in which message represented by integers are raised to a given power and only the residues modulo a preselected encryption modulus is transmitted from sender to receiver.

For example if the message is 7, the encryption key is 3 and the modulus is 10, then the transmitted message would not be $7^3 = 343$, but only the digit : 3. Chapter 5 and chapter 8 are devoted to the topic cryptography and primality and factoring, which contains the application of Number theory to cryptography.

DISTRIBUTION OF PRIME NUMBERS

1.1. PRIME NUMBERS



PRIME NUMBERS AND DISTRIBUTION OF PRIME NUMBER

1.1. PRIME NUMBERS.

The numbers 1, 2, 3, are called positive integers. Among the positive integers there is as subclass of peculiar importance, the class of primes. A number p is said to be prime if

(i) $p > 1$

(ii) p has no positive divisor except 1 and p .

NOTE An integer a is said to be divisible by another integer b , not 0, if there is a third integer c such that

$$a = b c.$$

In this case b is said to be a positive proper divisor of a .

A number greater than 1 but not prime is called as composite .

Example : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47 are the primes less than 50.

Now the question is how to find out the primes. The process is known as primality test . The first elementary test is sieve method

SIEVE OF ERATOSTHENES : In order to find prime number between 1 and 100 we proceed as follows:

STEP 1 : Write the numbers 1 to 100 in tabular form from 1 to 6 in column 1, 7 to 12 in column 2 and so on then proceed step by step

STEP 2 : Consider the second row starting with 2 strike out all multiples of 2 in the table and round 2.

STEP 3 : Consider third row starting with 3 and strike out all multiples of 3 from the table and round 3.

STEP 4 : Take 5th row starting with 5. Strike out all multiples of 5 from the rest of numbers in the table excepts 5. Round 5.

STEP 5 : Round the numbers left out in the table after following step 2 to step 4.

These are the numbers which are prime numbers between 1 and 100. 1 is not considered as a prime number though it is divisible by 1 and so there are 25 primes between 1 to 100. If you are asked to find out primes between 100 to 200 the same procedure is repeated Here one has to consider the multiples of 7, 11 and so on. This process is most elementary and can not be tried with a very big number with 10 million digits.

The following BASIC programme computes all the prime numbers upto 1000 using the sieve of Erastosthenes.

```

100      REM SIEVE OF ERATOSTHENES
110      DIM N [1000], P[200]
120      FOR I = 2 TO 1000
130          LET N [I] = 0
140      NEXT I
150      LET K = 0
160      FOR P = 2 TO 1000
170          IF N[P] < 0 THEN 240
180          LET K = K + 1
190          LET P[K] = P
200          IF P > SQR (1000) THEN 240
210          FOR I = P TO 1000 STEP P
220              LET N[I] = -1
230          NEXT I
240      NEXT P
250      REM PRINT PRIME NUMBERS
260      LET C = 1
270      FOR I = 1 TP K
280          PRINT P[I];
290      LET C = C+1

```

```

300      IF C <= 7 THEN 330
310      PRINT
320      LET C = 1
330      NEXT I
340      END
    
```

RUN

2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61
67	71	73	79	83	89	97	101	103
107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251
257	263	269	271	277	281	283	293	307
311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419
421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643
647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827
29	839	853	857	859	863	877	881	883
887	907	911	919	929	937	941	947	953
967	971	977	983	991	997			

THEOREM 1 : Every positive integer except 1, is a product of primes.

PROOF : Either n is a prime, when there is nothing to prove; or n has divisors between 1 and n . If n is composite then there exists an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d choose p_1 to be the smallest. Then p_1 must be a prime number otherwise it would have a divisor q with $1 < q < p_1$, but then $q \mid p_1$, and $p_1 \mid n$ imply $q \mid n$ which contradicts the choice of p_1 as the smallest divisor not equal to 1.

We write $n = p_1 n_1$, where p_1 is a prime and $1 < n_1 < n$. If n_1 is prime we are done. Otherwise the process is repeated to find another prime p_2 such that $n_1 = p_2 n_2$, that is

$$n = p_1 p_2 n_2 \quad 1 < n_2 < n_1.$$

Repeating the argument we have now

$$(1) \quad n = p_1 p_2 p_3 \dots p_k.$$

1.2. GREATEST COMMON DIVISOR :

If d divides two integers a and b , then d is called a common divisor of a and b .

THEOREM 2 : Given any two integers a and b , there is a common divisor d of a and b of the form

$$(2) \quad d = ax + by$$

where x and y are integers. Moreover, every common divisor of a and b divides this d .

PROOF : First we assume that $a \geq 0$ and $b \geq 0$.

We use induction on n ; where $n = a + b$. If $n = 0$ then $a = b = 0$ and we take $d = 0$ with $x = y = 0$. Assume the theorem is true for $0, 1, 2, \dots, n-1$. To prove it for n , assume $a \geq b$. If $b = 0$ take $d = a$, $x = 1$, $y = 0$. If $b \geq 1$ apply the theorem to $a - b$ and b . Since $(a - b) + b = a = n - b \leq n - 1$, by induction hypothesis there is a common divisor d of $(a - b)$ and b of the form $d = (a - b)x + by$. This d also divides $a - b + b = a$ so d is a common divisor of a and b , and we have $d = ax + (y - x)b$, a linear combination of a and b . Since a common divisor divides a and b and hence by linearity it divides d . Hence proved.

If $a < 0$ or $b < 0$ (or both), we can apply the result to $|a|$ and $|b|$. Then there is a common divisor d of $|a|$ and $|b|$ of the form

$$d = |a| x + |b| y$$

If $a < 0$, $|a| x = -a x = a(-x)$. Similarly $b < 0$, $|b| y = b(-y)$. Hence d is again a linear combination of a and b .

Definition : (Greatest common divisor)

Given integers a and b , there is one and only one number d with the following properties :

(a) $d \geq 0$

(b) $d \mid a$ and $d \mid b$

(c) $e \mid a$ and $e \mid b$ implies $e \mid d$.

Then d is called as the greatest common divisor (\gcd) of a and b and is denoted by (a,b) . $\gcd(-10, 34) = 2$. If $d = (a,b) = 1$ then a and b are said to be relatively prime.

By theorem 2, there exists integers x and y such that $1 = ax + by$.

Corollary 1 : If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

PROOF : Since $\gcd(a, b) = d$ it is possible to find integers x and y such that $d = ax + by$. Dividing each side of this equation by d , we get the expression

$$1 = (a/d)x + (b/d)y.$$

Because a/d and b/d are integers then $(a/d, b/d) = 1$, i.e. a/d and b/d are relatively prime.

Corollary 2 : If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

PROOF : As $a \mid c$ and $b \mid c$ we can find integers r and s such that $c = ar = bs$. Now $\gcd(a,b) = 1$ allows us to write $1 = ax + by$ for some integers x and y . Multiplying by c we get

$$c = c.1 = c(ax + by) = acx + bcy.$$

Substituting values of c on the right hand side, we get

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

which implies that $ab \mid c$.

THEOREM 3 : (Euclid's lemma) If $a \mid bc$ and if $(a,b) = 1$, then $a \mid c$.

PROOF : Since $(a,b) = 1$, we can write by theorem 2, $1 = ax + by$. Therefore $c = acx + bcy$. But $a \mid acx$ and $a \mid bcy$, so $a \mid acx + bcy = c$. Hence proved.

Remark: $\gcd(a,b) = 1$ is a necessary condition for theorem 3. For Example $15 \mid 6 \cdot 10$ but $15 \nmid 6$ and $15 \nmid 10$.

THEOREM 4 : If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

PROOF : If $p \mid a$ then we need not go further. So let us assume that $p \nmid a$. Since the only positive divisors of p are 1 and p itself, this implies that $\gcd(p,a) = 1$. But $\gcd(p,a) = p$ or $\gcd(p,a) = 1$ according as $p \mid a$ or $p \nmid a$. Since $p \mid ab$ and $p \nmid a$ by Euclid lemma we get $p \mid b$.

Corollary 3. If p is a prime and $p \mid a_1, a_2, \dots, a_n$ then $p \mid a_k$ for some k , where $1 \leq k < n$.

PROOF : We proceed by induction on n , the number of factors. When $n = 1$, conclusion is trivial. When $n = 2$ the result is theorem 4. Assume $n \geq 2$ and that whenever p divides a product less than n factors, then it divides at least one of its factors. Now let $p \mid a_1 a_2 \dots a_{n-1}$. According to theorem 1 $p \mid a_n$ or $p \mid a_1, a_2, \dots, a_{n-1}$. If $p \mid a_n$ then we are done. For the case $p \mid a_1 a_2 \dots a_{n-1}$ by induction hypothesis $p \mid a_k$ for k with $1 \leq k \leq n-1$. Hence p divides one of the integers a_1, a_2, \dots, a_n .

Corollary 4. If p, q_1, q_2, \dots, q_n are all primes and $p \mid q_1, q_2, \dots, q_n$ then $p \mid q_k$ for some k , where $1 \leq k < n$.

PROOF : By corollary 1, we know that $p \mid q_k$ for some k , with $1 \leq k \leq n$. Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself. Since $p > 1$, we conclude that $p = q_k$.

THEOREM 5 : (Fundamental Theorem of Arithmetic)

The representation of every integer $n > 1$ as a product of primes in (1) is unique apart from the order in which the factors occur.

PROOF : Let us suppose that the integer n can be represented as a product of primes in two ways say

$$n = p_1 p_2 p_3 \dots p_r = q_1 q_2 q_3 \dots q_s,$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 < \dots \leq p_r, \quad q_1 \leq q_2 \leq \dots \leq q_s.$$

Since $p_1 \mid q_1 q_2 \dots q_s$ then $p_1 = q_k$ for some k , but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Continuing we get if $r < s$

$$1 = q_{r+1} q_{r+2} \dots q_s$$

which is absurd, since each $q_i > 1$ hence $r = s$ and

$$p_1 = q_1, p_2 = q_2, \dots, p_r = q_r$$

giving the uniqueness of the two representations of n .

Any positive integer $n > 1$ has canonical form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

$$(3) \text{ or } n = \prod_{i=1}^r p_i^{\alpha_i}, \text{ where } p_1 \leq p_2 \leq \dots \leq p_r, \alpha_i' s \geq 0.$$

This is called as the standard form of n .

THEOREM 6 : If $n = \prod_{i=1}^r p_i^{a_i}$, the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^r p_i^{c_i}$, where $0 < c_i \leq a_i$, for $i = 1, 2, \dots, r$.

PROOF : For $0 \leq c_i \leq a_i$ $p_i^{c_i}$ divides $p_i^{a_i}$.

$$\text{So } \prod_{i=1}^r p_i^{c_i} \text{ divides } \prod_{i=1}^r p_i^{a_i}.$$

THEOREM 7 : If two positive integers a and b have the factorization

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, b = \prod_{i=1}^{\infty} p_i^{b_i}, \text{ then their gcd has the factorization}$$

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i},$$

$$\text{where } c_i = \min \{a_i, b_i\},$$

PROOF : Let $d = \prod_{i=1}^{\infty} p_i^{c_i}$. Since $c_i \leq a_i$ and $c_i \leq b_i$ we have d divides a and d divides b so d is a common divisor of a and b . Let e be a common divisor of a and b , and write e

$$e = \prod_{i=1}^{\infty} p_i^{e_i}. \text{ Then } e_i \leq a_i \text{ and } e_i \leq b_i, \text{ so } e_i \leq c_i,$$

Hence $e \mid d$. So d is the gcd of a and b .

Euclidean Algorithm

We describe the Euclidean Algorithm as follows : Let a and b be two integers whose greatest common divisor is desired. Since $\gcd(|a|, |b|) = \gcd(a, b)$ there is no harm in assuming that $a \geq b > 0$. By division algorithm we find integers q_1 and r_1 such that

$$a = q_1 b + r_1 \quad 0 \leq r_1 < b.$$

If it happens that $r_1 = 0$ then $b \mid a$ and $\gcd(a, b) = b$ when $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then we stop; otherwise, proceeding as before we obtain

$$r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2.$$

This division process continues until some zero remainder appears, say at the $(n+1)$ the stage where r_{n-1} is divided by r_n .

We get a decreasing sequence $b > r_1 > r_2 > \dots \geq 0$ satisfying the following system of equation :

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2$$

.

.

$$r_n = q_n r_{n-1} + r_n, \quad 0 < r_{n-2} < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0 \quad 0 < r_n < r_{n-1}.$$

Now $r_n = \gcd(a, b)$.

Since if $d = \gcd(a, b)$ then $d \mid a$ and $d \mid b$ imply that $d \mid (a - q_1 b)$ or $d \mid r_1$ by the relation $a = q_1 b + r_1$. Thus d is a common divisor of both b and r_1 . if c is a common divisor of b and r_1 then $c \mid q_1 b + r_1 = a$. So c is a common divisor of both a and b . Hence $c \leq d$. It now follows from the definition of $\gcd(b, r_1)$ that $d = \gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_n, 0) = r_n$. hence r_n is the greatest common divisor of integers a and b . We can express r_n as a linear combination of a and b .

Example 1. Find $\gcd(1998, 2000)$.

$$2000 = 1998 \times 1 + 2$$

$$1998 = 2 \times 999 + 0$$

Hence $\gcd(1998, 2000) = 2$.

We express 2 as a linear combination of 1998 and 2000.

$$2 = 2000 \times 1 + 1998 (-1).$$

Example 2. Find $\gcd(143, 227)$.

$$227 = 143 \times 1 + 84$$

$$143 = 84 \times 1 + 59$$

$$84 = 59 \times 1 + 25$$

$$59 = 25 \times 2 + 9$$

$$25 = 9 \times 2 + 7$$

$$9 = 7 \times 1 + 2$$

$$7 = 2 \times 3 + 1$$

$$2 = 1 \times 2 + 0$$

Hence $\gcd(143, 227) = 1$.

We express 1 as a linear combination of 143 and 227.

$$1 = 7 - 6$$

$$= 7 - 2 \times 3$$

$$= 7 - 3(9 - 7)$$

$$= 4 \times 7 - 3 \times 9$$

$$= 4 \times (25 - 9 \times 2) - 3 \times 9$$

$$= 4 \times 25 - 11 \times 9$$

$$= 4 \times 25 - 11(59 - 25 \times 2)$$

$$= 26 \times 25 - 11 \times 59$$

$$= 26 \times (84 - 59) - 11 \times 59$$

$$= 26 \times 84 - 37 \times 59$$

$$= 26 \times 84 - 37 \times (143 - 84)$$

$$= 63 \times 84 - 37 \times 143$$

$$= 63 \times (227 - 143) - 37 \times 143$$

$$= (6 \times 3) 227 - (100) 143.$$

The \gcd of 76084 and 63020 is 92.

The following BASIC program uses Euclid's algorithm to compute the \gcd of given pair of numbers.

```

100  REM FIND THE GCD OF TWO NUMBERS
120  PRINT"  A","  B"," GCD "
130  PRINT
140  READ A,B
150  PRINT A,B
160  LET Q = INT (A/B)
170  LET R = A - Q * B
180  LET A = B

```

```

190   LET B = R
200   IF R > 0 THEN 160
210   PRINT A
220   GPTP 140
230   DATA 60, 5280, 49, 139, 3850, 5280
240   DATA 1124, 1472, 17296, 18416
250   DATA 76084, 63020, 7854, 13398
260   END

```

RUN

A	B	GCD :	60	5280	60,	49	139	1,
3850	5280	110,	1124	1472	4,	17296	18416	16
76084	63020	92,	7854	13398	462.			

OUT OF DATA IN LINE 140.

1.3. HOW MANY PRIME NUMBERS ARE THERE ?

THEOREM 8 : If n is a natural number > 2 then between n and $n!$ there is at least one prime number.

PROOF : As $n > 2$, the integer $N = n! - 1$ is > 1 and, it has a prime divisor p , which is obviously $\leq N$ and so $< n!$. Now we can not have $p \leq n$, because then p would be a divisor of the number $n!$, and being also a divisor of the number N , it would be a divisor of the differences of these numbers, i.e. the numbers $n! - N = 1$ which is impossible. Therefore $p > n$ and as we know, $p < n!$ we have $n < p < n!$ and the theorem is proved.

In connection of the above theorem we observe that in 1850 Chebyshev proved a stronger theorem called as Bertrand postulate:

Between n and $2n$ there exists at least one prime p . That is $n \leq p < 2n$.

Therefore, for every natural number there exists a prime number greater than that number, whence it follows that there are infinite number of primes which was known to Euclid.

THEOREM 9 : (Euclid) There are infinite number of primes.

PROOF : Suppose that there are only a finite number, say $p_1 p_2 \dots p_n$. Let $N = 1 + p_1 p_2 \dots p_n$. Now $N > 1$, so either N is prime or N is a product of primes. N is not prime since it exceeds each p_i . Moreover no p_i divides N . Because if p_i divides N , then p_i divides the difference $N - p_1 p_2 \dots p_n = 1$. This is a contradiction. This proves the theorem.

Second proof of Euclid's theorem: Suppose that $2, 3 \dots p_j$ are the first j primes and let $N(x)$ be the number of n not exceeding x which are not divisible by any prime $p > p_j$. If we express such an n in the form

$$n = n_1^2 m,$$

where m is 'quadrifrei' i.e. is not divisible by the square of any prime, we have

$$m = 2^{b_1} 3^{b_2} \dots p_j^{b_j}$$

with every b either 0 or 1. There are just 2^j possible choices of the exponents and so not more than 2^j different values of m . Again $n_1 < \sqrt{n} \leq \sqrt{x}$ and so there are not more than \sqrt{x} different values of n_1 . Hence

$$(4) \quad N(x) \leq 2^j \sqrt{x}.$$

If the theorem is false, so that the number of primes is finite, let the primes be $2, 3, \dots, p_j$. In the case $N(x) = x$ for every x and so $x \leq 2^j \sqrt{x}$ implies $x \leq 2^{2j}$ which is false for $x \geq 2^{2j} + 1$.

THEOREM 10 : The infinite series $\sum_{n=1}^{\infty} 1/p_n$ is divergent.

PROOF : We will use the above argument for the proof of this theorem. If the series is convergent, we can choose j , so that the remainder after j terms is less than $1/2$ i.e.

$$(5) \quad \frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} = \dots < \frac{1}{2}$$

The number $n \leq x$ which are divisible by p are at most x/p . Hence $x - N(x)$, the number of $n \leq x$ divisible by one or more $p_{j+1}, p_{j+2} \dots$ is not more than

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} = \dots < \frac{1}{2} x$$

Hence by (4)

$$1/2 x < N(x) < 2^j \sqrt{x}$$

i.e.

$$x < 2^{2j+2}, \text{ which is false for } x \geq 2^{2j+2}.$$

Hence the series diverges.

THEOREM 11 : There are infinitely many primes of the form $4n-1$.

PROOF : Define N by $N=2^2.3.5 \dots p-1$. Then N is of the form $4n-1$ and is not divisible by any of the primes upto p . It can not be a product of primes of the form $4n+1$ only, since the product of two numbers of this form is of the same form; and therefore it is divisible by a prime $4n-1$ greater than p . Hence there are infinitely many primes of the form $4n-1$.

THEOREM 12 : There are infinitely many primes of the form $4n+3$.

PROOF Define N by $N=2^2.3.5\dots p-1$ Then N is of the form $4n+3$, and is not divisible by any of the primes upto p . It can not be a product of primes $4n+1$ only, since the product of two numbers of this form is of the form $4n+1$; and therefore it is divisible by a prime $4n+3$, greater than p . Hence there are infinitely many primes of the form $4n+3$.

THEOREM 13 : There are infinitely many primes of the form $6n+5$.

PROOF : The proof is similar. Define N as $N=2 \cdot 3 \cdot 5 \dots p-1$.

We observe that any prime numbers, except 2 or 3, is $6n-1$ or $6n+5$ and the product of two numbers of the form $6n+1$ is the of the same form. Hence prime divisors of N are of the form $6n+5$ greater than p . Hence there are infinitely many primes of the form $6n+5$.

THEOREM 14 : There are infinitely many primes of the form $8n+5$.

PROOF : We take $N=3^2, 5^2, 7^2 \dots p^2+2^2$, a sum of two squares which have no common factor. The square of an odd number $2m+1$ is $4m(m+1)+1$ and is $8n+1$. So that N is $8n+5$. By above theorem any prime factor of N is $4n+1$, and so $8n+1$ or $8n+5$ and that the product of two numbers $8n+1$ is of the same form, we complete the proof as before.

THEOREM 15 : If p_n is the n^{th} prime number, then $p_n \leq 2^{2^{n-1}}$.

PROOF : Let us proceed, by induction on n . For $n=1$, it is trivial. Assume $n > 1$ and that the result holds for integers up to n . Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \dots p_n + 1 \\ &\leq 2 \cdot 2^2 \dots 2^{2^{n-1}} + 1 = 2^1 + 2^2 + \dots + 2^{2^{n-1}} + 1 \\ &\leq 2^{2^n - 1} + 1 \end{aligned}$$

But $2^{2^n - 1} \geq 1$ for all n ; whence

$$p_{n+1} \leq 2^{2^n - 1} + 2^{2^n - 1} = 2 \cdot 2^{2^n - 1} = 2^{2^n}$$

Hence proved.

Corollary : For $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n} .

PROOF : From the theorem we know that p_1, p_2, \dots, p_n are all less than 2^{2^n} .

There exist prime numbers having at least three thousand digits, but no such number is known. The greatest known prime number has 1332 digits it is the number $2^{4423}-1$ which was verified to be prime in the year 1961. Most recently largest known prime is $2^{6,972,593}-1$ having 2, 098, 960 digits found by Nayan Hajaratwala in June 1999.

From Bertrands postulate it follows that for every natural number there exist at least three prime numbers each having s digits. Since each of the numbers

$$10^{s-1}, 2 \cdot 10^{s-1}, 4 \cdot 10^{s-1} \text{ and } 8 \cdot 10^{s-1}$$

have s digits, then for $s > 1$ there exist prime numbers p, q and r such that

$$10^{s-1} < p < 2 \cdot 10^{s-1} < q < 4 \cdot 10^{s-1} < r < 8 \cdot 10^{s-1};$$

it is clear that each of the numbers p, q, r has s digits.

For $s = 1$, we have four primes of one digit 2, 3, 5 and 7. The number of two digits primes is twenty-one, of three digit primes is 143. Thus there exist at least three prime numbers of a hundred digits each. R.M. Robinson has found three prime numbers of a hundred digits.

$$81 \cdot 2^{324} + 1, 63 \cdot 2^{326} + 1, 35 \cdot 2^{327} + 1.$$

We do not know so far any prime number having a thousand digits, although we known there exist atleast three such numbers. Such prime numbers are called as Titanic primes.

1.4. TWIN PRIMES :

There arises a series of questions about the infinite sequence of consecutive prime numbers, i.e. the sequence 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... only some of there question can be answered easily.

The smallest two prime numbers are 2 and 3. These are successive natural numbers. the question arises: if there are other successive natural number which are both prime; the answer is no. Because of two successive natural numbers one is even, and if it is >2 then it is composite.

There are many pairs of successive odd numbers which are both primes, for example 3 and 5, 5 and 7, 11 and 13, 17 and 19, 29 and 31, 41 and 43. We call such pairs twin primes. There are 152, 892 such pairs of numbers less than 30 million.

The following BASIC program computes and prints all twin primes less than 1000.

```

100      REM TWIN PRIMES LESS THAN 1000
120      DIM A [1000], B [400]
120      FOR X = 2 TO 1000
130      LET A [X] = 0
140      NEXT X
150      LET C = 0
160      LET S = SQR (1000)
170      FOR B = 2 TO 1000
180      IF A [B] < 0 THEN 250
190      LET C = C + 1
200      LET B[C] = B
210      IF B>S THEN 250
220      FOR X = B TO 1000 STEP B
230      LET A [X] = -1
240      NEXT X
250      NEXT B
260      PRINT "TWIN PRIMES"
270      PRINT
280      FOR X = 2 TO C
290      IF B[X] - B[X-1] <> 2 THEN 310
300      PRINT B[X-1]; B [X]
310      NEXT X
320      END

```

RUN

TWIN PRIMES

3	5
5	7
11	13
17	19
29	31
41	43
59	61
71	73

101	103
107	109
137	139
149	151
179	181
191	193
197	199
227	239
269	271
281	283
311	313
347	349
419	421
431	433
461	463
521	523
569	571
599	601
617	619
641	643
659	661
809	811
821	823
827	829
857	859

Long ago the question was asked whether the number of twin primes is infinite. We do not know the answer to this question.

Twin prime conjecture : There are infinitely many prime pair $p, p+2$. The argument which makes it plausible that

$$(6) \quad P_2(x) \sim \frac{2c_2x}{(\log x)^2}$$

where $P_2(x)$ is the number of these pairs with $p \leq x$ and

$$c_2 = \prod_{p>2} \left\{ \frac{p(p-2)}{(p-1)^2} \right\} = \prod_{p \geq 3} \left\{ 1 - \frac{1}{(p-1)^2} \right\}.$$

It is an unanswered question whether there are infinitely many pair of twin primes that is, pairs of successive odd integers p and $p+2$ which are both primes. Electronic computers have discovered 152,892 pairs of twin primes less than 30,000,000 and twenty pairs between 10^{12} and $10^{12}+10,000$. The largest to date twin primes are $107570463 \cdot 10^{2250} \pm 1$ each 2259 decimal digits long were discovered in 1985.

The largest known pairs of twin primes are $1706595 \times 2^{11235} \pm 1$ and $571305 \times 2^{7701} \pm 1$ found in 1990 by B. Parady, J. Smith and S. Zarantonello. In 1998, Ray Ballinger found the largest twin primes $835335 \times 2^{39014} \pm 1$ having 11751 digits.

For every $x > 1$ let $\pi_2(x)$ denote the number of primes p such that $p+2$ is also prime and $p+2 \leq x$.

Brun announced in 1919 that there exists an effectively computable integer x_0 such that, if $x \geq x_0$, then $\pi_2(x) < 100x / (\log x)^2$. Further $\sum (1/p + 1/(p+2))$ converges which express scarcity of twin prime, even if there are infinitely many of them.

$$B = (1/3 + 1/8) + (1/5 + 1/7) + \dots + (1/p + 1/(p+2)) + \dots$$

is called Brun's constant and the value of B is 1.90216054.

Growth of $\pi_2(x)$

x	$\pi_2(x)$
10^3	35
10^4	205
10^5	1224
10^6	8169
10^7	58980
10^8	440312
10^9	3424506
10^{10}	27412679

Record : The largest exact value for the number of twin primes below a given limit has been published by Brent in 1976.

$$\pi_2(10^{11}) = 224,376,048.$$

Now the question is: which digits can there be at the beginning and at the end of a prime number?

The last digit of a prime number having more than one digit can not be even because then the number would be >2 and thus even and composite; the last digit can not be 5 because then the number would be greater than 5 and

divisible by 5 and so it would be composite. Thus the last digit of a prime number >10 can only be 1, 3, 7 and 9.

There exists prime number having at the beginning and at the end an arbitrary large number of digits equal to 1 (but the middle digit may be other than 1).

In this connection the problem arises whether there exist infinitely prime numbers whose digits are all 1, for example 11 and

$$11,111,111,111,111,111,111,111, = (10^{23} - 1) / 9.$$

Such type of numbers are called as Repunits. Repunits having 9 ones is prime.

The proof that the last number is prime is not easy. However it is easy to prove that, if a number whose digits are all 1 is prime then the number of its digits must be prime. This property, however, is not sufficient because, for example,

$$111 = 3 \times 37; 11,111 = 41 \times 271; 1,111,111 = 239 \times 4649.$$

Also the number $(10^{37}-1)/9$ having thirty seven digits is composite and the number $(10^{641}-1)/9$ having 641 digits is composite and divisible by 1238.

Prime numbers other than those formed by the same digits have been found which remain prime after every permutation of their digits, for example 13,113. It is not known whether these numbers are finite.

Also we do not know if there exist infinitely many prime numbers whose first and last digits are 1 and the remaining ones are 0, as for example the number 101. It is easy to prove that such a prime number must be of the form $10^{2^n} + 1$ where n is natural number, but again this property is not sufficient because $10^{2^2} + 1 = 73 \times 137$ we can not answer the question whether the sequence of sums of the digits of consecutive prime number tend to infinity.

1.5. CONJECTURE OF GOLDBACH

In 1742, Christian Goldbach stated conjecture that each even number >2 is the sum of two primes This conjecture still remains neither proved nor disproved. A stronger conjecture has been made, namely that every even number >6 is the sum of two distinct prime numbers and this is verified for numbers $<100,000$.

• It can be proved that the last conjecture is equivalent to the statement that every natural number >17 is the sum of three different primes for example $19 = 3+5+11$. A. Schinzel has proved that the conjecture of Goldbach implies that

every odd number > 17 is the sum of three different primes. Every even integer greater than 4 can be written as a sum of two odd prime numbers.

Example :

$$10 = 3 + 7 = 5 + 5$$

$$22 = 3 + 19 = 5 + 17 = 11 + 11$$

$$30 = 7 + 23 = 11 + 19 = 13 + 17.$$

THEOREM 16 : Every odd number > 7 is the sum of three odd primes.

PROOF : From the conjecture of Goldbach this follows easily. If n is a natural number and $2n + 1 > 7$ then $2n + 1 - 3 = 2(n-1) > 4$. The even number $2(n-1) > 4$ is, by the conjecture of Goldbach, the sum of two prime p and q , which can not be even, because our number is > 4 . The prime numbers p and q are therefore odd and the number $2n + 1 = 3 + p + q$ is the sum of three odd primes.

We do not know whether every odd number > 7 is the sum of three odd primes, but in 1937, I. Vinogradov proved that every sufficiently large odd number is the sum of three odd primes. We know a number $a = 3^{3^{15}}$ which is the sum of three odd primes.

THEOREM 17 (Euler) :

The following two statements are equivalent.

(A) Every integer $n > 5$ is the sum of three primes.

(B) Every even integers $2n \geq 4$ is the sum of two primes.

PROOF : Assume that (B) holds and if $2n \geq 6$, then $2n - 2 = p + p'$ so $2n = 2 + p + p'$, where p, p' are primes. Also $2n + 1 = 3 + p + p'$ which proves (A).

Conversely, if (A) is assumed to be true and if $2n \geq 4$, then $2n + 2 = p + p' + p''$ with p, p', p'' primes, then necessarily $p'' = 2$ (say) and $2n = p + p'$.

Note that it is trivial that (B) is true for infinitely many even integers

$$2p = p + p \text{ (for every prime).}$$

Further it has been proved that every natural number > 11 is the sum of two or more different primes. For example $12 = 5 + 7$, $13 = 2 + 11$, $17 = 2 + 3 + 5 + 7$, $29 = 3 + 7 + 19$. A Makowski has proved that every natural number > 55 is the sum of different primes of the form $4k + 3$.

THEOREM 18 : Every odd (positive or negative) integer can be written in an infinite number of ways in the form $p + q - r$ where p, q and r are odd primes.

PROOF : For every integer k there exists an odd prime number r such that $2k - 1 + r > 4$. (It is enough to take for r a sufficiently large prime number). But then $2k - 1 + r$ is an even number > 4 , therefore, by Goldbach's conjecture

$2k - 1 + r = p + q$, where p and q are odd prime numbers. Hence $2k - 1 = p + q - r$ in which the prime number r may be arbitrarily large. Hence proved.

THEOREM 19 : Every natural number > 11 is the sum of two composite numbers.

PROOF : If $n > 11$ is an even number, then $n - 4$ is an even number > 2 , i.e. the sum of two composite numbers. But if $n > 11$ is odd then $n - 9$ is an even number > 2 , i.e. it is composite and $n = (n - 9) + 9$, i.e. the sum of two composite number

Remark : From the above theorem we should not conclude that the inquiry into composite numbers is easier than investigations about prime numbers, for it is still unanswerable whether or not among numbers $F_n = 2^{2^n} + 1$, $n = 1, 2, 3, \dots$ we have infinitely many composite numbers. We only know thirty eight such composite number of which the greater is F_{1945} .

G.H. Hardy and J. E. Littlewood conjectured that every sufficiently large natural number which is not a perfect square is the sum of a square of an integer and a prime number.

THEOREM 20 : There exist infinitely many squares of natural numbers which are , as also those which are not the sum of a prime number and the square of an integer.

PROOF : If p is an odd prime, then $(p + 1) / 2$ is a natural number and we have

$$\left(\frac{p+1}{2}\right)^2 = \left(\frac{p-1}{2}\right)^2 + p$$

On the other hand if $n = 3k + 2$, where k is a natural number, then for some integer x and a prime number p we can not have,

$$n^2 = x^2 + p,$$

for then n would be $.x$ and

$$p = n^2 - x^2 = (n + x)(n - x)$$

whence, considering that p is prime, $n - x = 1$ and $n + x = p$, so that

$$p = 2n - 1 = 3(2k + 1)$$

which is not possible for a natural number k .

1.6. FERMAT NUMBERS.

Fermat numbers are numbers of the form $F_n = 2^{2^n} + 1$, where $n = 0, 1, 2,$

.....

A famous mathematician of the seventeenth century, P. Fermat conjectured that all these numbers are prime. This is true for $n = 0, 1, 2, 3, 4$. But L. Euler in 1732 showed that the number,

$$F_5 = 2^{2^5} + 1 = 4,294,967, 297$$

having 10 digits is composite and divisible by 641. We know 38 composite numbers F_n , namely for $n=5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945$.

These 38 composite numbers F_n include those for which we know the prime factors (for example F_5 and F_6) those whose prime factor we do not know. The number of digits of the composite Fermat number F_{1945} is $>10^{582}$

- (1) The largest know Fermat prime is $F_4=65537$
- (2) The largest known composite Fermat number is F_{23471} (Keller 1984, Amonwin 1985) which has a factor $5 \times 2^{23473} + 1$ and more than 10^{7000} digits. Keller has also shown that F_{9448} is composite having the factor $19 \times 2^{9450} + 1$.

$F_{10} = 455925777 \times 6487031809 \times C_{291}$ where C_m denotes a composite number with m digits.

To find the prime divisor of F_n we know the following: Every natural divisor of the number F_n must be of the form $2^{2^{n+2}}k+1$, where k is an integer ≥ 0 . This can be verified by the following examples.

Example 1 : If $n = 1945$, the divisors of F_{1945} can only be in the arithmetic progression $2^{1947}k + 1$ ($k = 0, 1, 2, \dots$). For $k = 0$ we obtain the trivial divisor 1. For $k = 1$, the number $2^{n+2} + 1 = 2^{1947} + 1$ is obviously divisible by 3 and so is not a prime. For $k = 2$, the number $2^{n+2} \cdot 2 + 1 = 2^{1948} + 1 = (2^4)^{487} + 1$ is divisible by $2^4 + 1$ and so is not prime. For $k = 3$, the number $2^{n+2} \cdot 3 + 1 = 2^{1947} \cdot 3 + 1$ is composite, divisible by 5 because $5 \mid 2^4 - 1$ when $5 \mid 2^{1944} - 1$ and if we multiply the right side by $2^3 \cdot 3$, $5 \cdot 2^{1947} \cdot 3 - 24$, whence $5 \mid 2^{1947} \cdot 3 + 1$. For $k = 4$, the number $2^{n+2} \cdot 4 + 1 = 2^{1949} + 1$ is divisible by 3 and so is composite.

Thus trying to find the prime divisor of the number F_{1945} , we must divide it by $2^{1947} \cdot 5 + 1 = m$. As the division turns out to be without remainder, it follows that m is the smallest divisor of F_{1945} is a prime.

Example 2 : The divisor of F_5 is $2^7 \cdot k + 1$ that is $128k + 1$. For $k = 1$, we get 129 which is composite. For $k = 2$ we get 257 which is a prime but does not divide $F_5 = 4,294,467,297$. For $k = 3$ we get 385 which is composite. For $k = 4$ we get $513 = 2^9 + 1$ is divisible by 3 hence composite. For $k = 5$ we get the prime number 641 which divides F_5 . Dividing F_5 by 641 we get the quotient

6,700,417 which is also a prime. If F_5 is composite it must have a prime divisor not greater than its square root and so less than 2600. So we have $128k + 1 < 2600$ whence $k < 21$. For F_6 the prime divisor is $2^8 \cdot 1071 + 1$. Thus F_6 is composite.

THEOREM 21 : If $a \geq 2$ and $a^n + 1$ is prime, then a is even and $n = 2^m$.

PROOF: For if a is odd then $a^n + 1$ is even and if n has an odd factor k and $n = kl$, then $a^n + 1$ is divisible by $a^l + 1$ and

$$\frac{a^{kl} + 1}{a^l + 1} = a^{(k-1)l} - a^{(k-2)l} + \dots + 1$$

Hence $n = 2^m$. Hence proved.

THEOREM 22 : If F_n is prime, the number $3^{2^{n-1}} + 1$ is divisible by F_n .

For the proof of this theorem we require the following lemma.

LEMMA : If k is a nonnegative integer and the number $p = 12k + 5$ is prime, then the number $3^{6k+2} + 1$ is divisible by p .

PROOF : The lemma is true for the number $k = 0$; we may therefore say that k is a natural number. Let $p = 12k + 5$. We consider the product of the first $6k + 2$ natural numbers divisible by 3 and divide the factors of the product of three groups, putting in the first group the first $2k$ factors, in the second next $2k + 1$ factors and in the third the remaining $2k + 1$ factors.

First group gives the product $3 \cdot 6 \cdot 9 \dots 6k$.

The second group gives the product $(12k + 3) 12k (12k - 3) \dots (6k + 6) (6k + 3)$

(Changing the order of factors) which, since $p = 12k + 5$, can be written in the form

$$(p-2) (p-5) (p-8) \dots [p - (6k + 2)].$$

Because the number of divisors is odd i.e. $2k + 1$, our product, after expanding and collecting the terms divisible by p , gives us the number $p u - 2 \cdot 5 \cdot 8 \cdot (6k + 2)$, where u is a certain integer.

The factors of third group give the product

$$\begin{aligned} & (12k + 6) (12k + 9) (12k + 12) \dots (18k + 6) \\ &= (p+1) (p+4) (p+7) \dots (p+6k+1) \\ &= p v + 1 \cdot 4 \cdot 7 \cdot \dots \cdot (6k + 1) \end{aligned}$$

where v is a natural number.

We have now

$$\begin{aligned}
 & 3.6.9 \dots (18k+6) \\
 &= 3.6.9 \dots 6k (p-2.5.8 \dots (6k+2) (p-1.4.7 \dots (6k+1))) \\
 &= p w - 1.2.3.4.5.6 \dots (6k+1) (6k+2) \\
 &= p w - (6k+2)!
 \end{aligned}$$

where w is an integer.

$$\text{But } 3.6.9 \dots (18k+6) = (6k+2)! 3^{6k+2}$$

$$\text{i.e. } (6k+2)! 3^{6k+2} = p w - (6k+2)!$$

i.e. the number $p w$ is divisible by $(6k+2)!$, and so

$$p w = (6k+2)! t,$$

where t is an integer. But $6k+2 < 12k+5 = p$, and so the number $(6k+2)!$ is not divisible by p . As the product $(6k+2)! t$ is divisible by p , t must be divisible by p , $t = p s$, where $w = (6k+2)! s$, where s is an integer. Hence $3^{6k+2} = ps - 1$, when it follows that the number $3^{6k+2} + 1$ is divisible by p . Hence proved.

PROOF OF THE THEOREM 22 : Let n be a given natural number. We have $2^n = 2^m$ where m is a natural number. Hence $F_n - 1 = 4^m$ from which it follows that the number $F_n - 5$ is divisible by 4. We have $F_n - 1 = 4^m = (3+1)^m = 3t + 1$, where t is a natural number. Hence $F_n - 5 = 3(t-1)$ which proves that $F_n - 5$ is divisible by 3, and since as we have shown it is divisible by 4, it is divisible by 12. So $F_n = 12k + 5$, where k is an integer. From the lemma it follows that if F_n is prime then $3^{6k+2} + 1 = 3^{(F_n-1)/2} + 1 = 3^{2^{n-1}} + 1$ is divisible by F_n . Hence proved.

Example : F_7 is composite.

To prove this it is enough to show that $3^{2^{127}} + 1$ is not divisible by $F_7 = 340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 457$. To find this we have to find the remainder of the division of $3^{2^{127}}$ by F_7 . The number 3^{2^7} has 61 digits and calculate the remainder r of its divisor by F_7 . The remainder r_1 of the division of r^2 by F_7 will be the division of 3^{2^8} by F_7 . Similarly the remainder r_2 of the division of r_1^2 by F_7 will be the remainder of division of 3^{2^9} by F_7 . Proceeding we arrive at the remainder r_{120} of the division of the $3^{2^{127}}$ by F_7 . In this way it is found that $r_{120} \neq 2^{2^7}$, whence it follows that the

number $3^{2^{127}} + 1$ is not divisible by F_7 . So by the theorem 22, F_7 is composite. For the number F_{16} , the smaller prime divisor is 2^{18} . $3150 + 1$ was found in 1953, and conjectured that all number of the sequence .

$$2+1, 2^2+1, 2^{2^2}+1, 2^{2^{2^2}}+1, \dots$$

are prime was disproved. We do not know, if in this sequence there are infinitely many prime numbers or infinitely many composite numbers.

1.7. PRIME NUMBERS OF THE FORM $n^n+1, n^{n^n}+1$ etc.

Like Fermat numbers discussed in § 1.6. the question arises how many prime numbers are there of the form $n^n + 1$, where n is a natural number and it must be

$$\geq F_{20} > 2^{2^{20}} > 2^{10^6} > 10^{3 \cdot 10^5}$$

So among the numbers $n^n + 1$, there are only three primes:

$$1^1 + 1 = 2, 2^2 + 1 = 5, 4^4 + 1 = 257.$$

Consider the number of the form $n^{n^n} + 1$.

We have $1^1 = 2, 2^{2^2} + 1 = 17$. As above we can prove that if the number $n^{n^n} + 1$, where n is a natural number > 1 , is a prime, then for same integer $r \geq 0$, we must have $n = 2^{2^r}$, so that

$$n^{n^n} + 1 = F_{r+2} \cdot r + 2^r$$

For $r = 0$, since $F_2 = 17$, for $r = 1$ the number F_3 is composite. For $r = 2$, F_{66} is composite. Hence we have

Among the numbers having not more than 10^{18} digits, there exist only two prime numbers of the form $n^{n^n} + 1$, where n is a natural number 2 and 17.

Now the question arises:

Among the numbers,

$$(A) \quad 2+3, 2^2+3, 2^{2^2}+3, \dots \text{ how many primes exist.}$$

The answer is that there are only a finite number of primes in the set (A).

Suppose that $n^n + 1$ is prime for natural number n . Each natural number n is of the form $n = 2^k \cdot m$, where k is an integer ≥ 0 , and m is an odd number.

If $m > 1$, then the number $n^n + 1 = \left(n^{2^k}\right)^m + 1$ would be $> n^{2^k} + 1$ and is divisible by $n^{2^k} + 1$, giving $n^n + 1$ to be composite. Therefore, m must be equal to 1. So $n = 2^k$.

If $k = 0$, then $n = 1$, and the number $n^n + 1$ is a prime. If $k > 0$, then $k = 2^r \cdot s$, r is an integer ≥ 0 and s is an odd number.

If $s > 1$, then $n^n + 1 = 2^{2^r \cdot s \cdot n} + 1$ is divisible by $\left(2^{2^r \cdot n}\right) + 1$, hence composite. Therefore, $s = 1$ and $k = 2^r$ and $n = 2^r$ and

$$n^n + 1 = 2^{2^r} \cdot 2^{2^r} + 1 = 2^{2^{r+2^r}} + 1 = F_{r+2^r}.$$

Hence, $n^n + 1$ is prime if F_{r+2^r} is prime.

For $r = 0$, since $F_1 = 5$ is prime we get $2^2 + 1 = 5$ is prime. For $r = 1$, since $F_3 = 257$ is prime we get the prime number $4^4 + 1 = 257$. For $r = 2$, F_6 is composite divisible by 2^8 . $1071 + 1$. We do not get n so that $n^n + 1$ is prime. For $r = 3$ since F_{11} is composite $n^n + 1$ is also composite. If, therefore besides the number 2, 5 and 257 there exist prime numbers of the form $n^n + 1$,

$$\text{then they must be } \geq F_{20} > 2^{2^{20}} > 2^{10^6} > 10^{3 \cdot 10^5}.$$

THEOREM 23 : Among the numbers $2^{2^2} + 5, 2^{2^{2^2}} + 5, \dots$ there are no primes, because each of these numbers is divisible by 7.

PROOF : For a natural number k , the number $2^{2^k} = (3+1)^k$ where divided by 3 gives the remainder 1, so $2^{2^k} = 3t + 1$, where t is a natural number.

$$\text{Hence } 2^{2^{2k}} + 5 = 2^{3t+1} + 5 = (7+1)^t 2 + 5 \text{ which is divisible by 7.}$$

THEOREM 24 : For Fermat numbers F_n and F_m , where $m > n \geq 0$, $\gcd(F_m, F_n) = 1$.

PROOF : Put $d = \gcd(F_m, F_n)$. Since Fermat numbers are odd integers, d must be odd. If

we set $x = 2^{2^n}$ and $k = 2^{m-n}$, then

$$\frac{F_m - 2}{F_n} = \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} + 1} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \dots$$

where $F_n \mid (F_m - 2)$. From $d \mid F_n$, it follows that $d \mid (F_m - 2)$. But $d \mid F_m$ implies $d \mid 2$.

But d is an odd integer and so $d = 1$. This proves the theorem.

THEOREM 25 : For $F_n = 2^{2^n} + 1$ we have $F_n \mid 2^{F_n} - 2$ ($n = 1, 2, 3, \dots$)

PROOF : By induction we can show that $2^n \geq n+1$ which implies that

$$2^{n+1} \mid 2^{2^n} \text{ and } 2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1$$

Therefore

$$\begin{aligned} F_n &= 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1 \mid 2^{2^{2^n} + 2} - 2 \\ &= 2^{F_n} - 2 \text{ and } F_n \mid 2^{F_n} - 2 \end{aligned}$$

Hence proved.

1.8. MERSENNE NUMBERS

Mersenne numbers are numbers of the form $M_n = 2^n - 1$, where $n = 1, 2, 3, \dots$. These numbers are interesting in two respects. Firstly the greatest known prime numbers are Mersenne numbers and secondly it gives rise to perfect number, that is those which are equal to the sum of their natural divisors less than those numbers themselves.

Since $1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1$, i.e. the Mersenne number is the sum of the first n terms of the G.P.

The following is the BASIC program for finding Mersenne number

```

100      REM MERSENNE PRIMES
110      PRINT "PRIME" "MERSENNE"
120      PRINT "NUMBER", "PRIMES"
130      PRINT
140      FOR K = 1 TO 8
150      READ P
160      LET M = 2↑P-1
170      PRINT P,M
180      NEXT K
190      DATA 2,3,5,7,13,17,19
200      END

```

RUN	
PRIME NUMBER	MERSENNE PRIMES
2	3
3	7
5	31
7	127
13	8191
17	131071
19	524287

THEOREM 26 : If n is composite then the number in M_n is composite

PROOF : If $n = a \cdot b$ where a and b are natural numbers > 1 , then $2^a - 1 > 1$ and $2^n - 1 = 2^{ab} - 1 > 2^a - 1$, and the number $2^{ab} - 1$ is divisible by $2^a - 1$, and so is composite. Therefore if the number M_n , where $n > 1$, is prime, then the number n must be prime, but the converse is not necessarily true because, for example

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89.$$

If p is a prime number, then each natural divisor of the number M_p must be of the form $2kp + 1$, where k is an integer ≥ 0 .

Many of the Mersenne numbers M_p , where p is a prime number, are composite. For example $47 \mid M_{23}$, $167 \mid M_{83}$, $263 \mid M_{131}$, $359 \mid M_{179}$.

Conjecture 1. Among the numbers M_p , where p is a prime number, there exists infinitely many which are composite.

M_n , for $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ and 4423 is prime.

Conjecture 2. If the Mersenne number M_n is a prime then the number M_{M_n} is also prime.

This is true for first four smallest Mersenne numbers, but for fifth Mersenne number $M_{13} = 8191$ it is not true because $M_{M_{13}} = 2^{8191} - 1$ is composite (Robinsen). The verification of this required one hundred hours work on an electronic computer. Again although M_{17} , M_{19} are prime $M_{M_{17}}$ and $M_{M_{19}}$ are composite.

Let $\sigma(N)$ denotes the number of positive divisors of N . If $\sigma(N) = 2N$ then N is said to be a perfect number. Example $N = 6$, $N = 28$ are perfect numbers.

The following BASIC program computes the first two perfect numbers.

```

10      FOR N = 2 TO 100
20      LET S = 0
30      FOR D = 1 TO N/2
40      IF INT (N/D) <> N/D THEN 60
50      LET S = S+D
60      NEXT D
70      IF S <> N THEN 90
80      PRINT N; "IS A PERFECT NUMBER"
90      NEXT N
99      END

```

RUN

6 IS A PERFECT NUMBER

28 IS A PERFECT NUMBER.

THEOREM 27 : All even perfect numbers are of the form $2^{p-1} M_p$, i.e. $2^{p-1} (2^p - 1)$ if $M_p = 2^p - 1$ is a prime number.

PROOF : Let N be a number such that $N = 2^{p-1} M_p = 2^{p-1} (2^p - 1)$.

To prove that N is a perfect number.:

If $\sigma(N)$ denotes the sum of the divisors of N , then

$$\begin{aligned}
 \sigma(N) &= \sigma(2^{p-1} (2^p - 1)) = \sigma(2^{p-1}) \sigma(2^p - 1) \\
 &= (2^p - 1) (2^{p-1} + 1) \\
 &= 2 (2^{p-1} (2^p - 1)) \\
 &= 2N.
 \end{aligned}$$

making N a perfect number.

Conversely assume that N is an even perfect number. We may write N as

$N = 2^{p-1} m$, where m is an odd integer. Then

$$\begin{aligned}
 (7) \quad \sigma(N) &= \sigma(2^{p-1} m) = \sigma(2^{p-1}) \sigma(m) \\
 &= (2^p - 1) \sigma(m)
 \end{aligned}$$

Since N is perfect

$$(8) \quad \sigma(N) = 2N = 2^p m.$$

Equating (7) and (8) $2^p m = (2^p - 1) \sigma(m)$

which is simply to say that $2^{p-1} \mid 2^p m$.

But 2^p-1 and 2^p are relatively primes, whence $2^p-1 \mid m$, say $m=(2^p-1)M$. Substituting in (8) we get.

$$2^p(2^p-1)M = (2^p-1)\sigma(m)$$

This implies $\sigma(m) = 2^p M$. Since m and M are both divisors of m (with $M < m$) we have $2^p M = \sigma(m) \geq m + M = 2^p M$

leading to $\sigma(m) = m + M$. The implication of this inequality is that m has only two divisors M and m itself. It must be that m is prime and $M = 1$, in other words $m = (2^p-1)M = 2^p-1$ is a prime number.

THEOREM 28 : If $a^k - 1$ is prime ($a > 0, k \geq 2$) then $a = 2$ and k is prime p .

PROOF : Now $a^k-1 = (a-1)(a^{k-1} + a^{k-2} + \dots + a + 1)$

$$a^{k-1} + a^{k-2} + \dots + a + 1 \geq a + 1 > 1.$$

Since a^k-1 is prime, $a-1 = 1$ so that $a = 2$.

If k were composite, then take $k = rs$, with $r > 1$ and $s > 1$.

$$\text{Thus } a^k-1 = (a^r)^s-1 = (a^r-1)(a^{r(s-1)} + a^{r(s-2)} + \dots + a^r + 1)$$

and each factor on the right is greater than 1.

But this violates the primality of a^k-1 , so k must be prime.

For $p = 2, 3, 5, 7$ the values 3, 7, 31, 127 of 2^p-1 are primes so that

$$2(2^2-1) = 6$$

$$2^2(2^3-1) = 28$$

$$2^4(2^5-1) = 496$$

$$2^6(2^7-1) = 8128.$$

All are perfect numbers, are even and end in the digit 6 or 8. No odd perfect number exists. As only 38 Mersenne primes are known, only 38 even perfect numbers are known till to day. The 31st Mersenne prime is M_{216091} . The largest known even perfect number, the 31st one is

$$P_{31} = 2^{216090} (2^{216091} - 1).$$

a number of 130,100 digits.

$P_{32} = 2^{756838} (2^{756839} - 1)$ has 455663 digits. Most recently the 38th Mersenne prime was discovered by Nayan Hajratwala in June 1999. The number is $2^{6,972,593} - 1$. Just as for Fermat numbers, there are many open problems about Mersenne numbers

- (1) Are there infinitely many Mersenne primes?
- (2) Are there infinitely many composite Mersenne numbers?

Fermat number is $F_n = 2^{2^n} + 1$ ($n \geq 0$) and a triangular number is $T_m = \frac{1}{2} m(m+1)$.

By a triangular number we mean the numbers, which are represented by vertices of a triangle. For example 1, 3, 6, 10, 15, 21, 28 are triangular numbers.

Exercise : Show that the only Fermat number which is also triangular number is 3.

Solution : If F_n is triangular then

$$2^{2^n} + 1 = \frac{1}{2} m(m+1)$$

$$\Rightarrow 2^{2^n} = \frac{1}{2} m(m+1) - 1$$

$$\Rightarrow 2^{2^n} + 1 = m(m+1) - 2 = m^2 + m - 2 = (m-1)(m+2).$$

Both $(m+2)$ and $m-1$ are power of 2 and the difference is 3, so $m=2$ is the only solution i.e. 3 is the only triangular number which is also a Fermat number.

A number a is a triangular number it is necessary that $1+8a$ should be a perfect square.

THEOREM 29 : No Fermat number other than 3 is a triangular number.

PROOF : $2^{2^n} + 1$ is a triangular number

$$\Rightarrow 1 + 8(2^{2^n} + 1), \text{ i.e. } 9 + 2^{2^n+3} \text{ is a perfect square.}$$

$$\text{Let } 9 + 2^{2^n+3} = M^2 \text{ and } 2^n + 3 = t, \text{ then } 2^t = M^2 - 9 = (M+3)(M-3)$$

(A) $\Rightarrow M+3=2^s$ and $M-3=2^l$ and $s+1=t$, l can not be equal to 0. Since if $l=0$, $2^s=7$ which is absurd since s is an integer.

Hence $s > l \geq 1$.

Eliminating M from (A) we get

$$6 = 2^s - 2^l = 2^l(2^{s-l} - 1)$$

$$\text{i.e. } 2^l = 2 \text{ or } l = 1, 2^{s-l} - 1 = 3.$$

Hence $s = 3$ and $t = 4$.

Since $2^n + 3 = 4 \Rightarrow n = 0$.

n can not have any value other than 0. Hence the result.

THEOREM 30 : All Mersenne numbers for which n is odd and greater than one can not be triangular number.

PROOF : Mersenne number is $2^n - 1$. In order that it will be a triangular number,

$1 + 8(2^n - 1)$ must be a perfect square.

That is $1 + 2^3(2^n - 1)$ i.e. $2^{n+3} - 7$ is a perfect square.

That is $2^{n+3} - 7 = M^2$.

If n is odd, $n + 3$ is even. Let $n + 3 = 2k$, then

$$2^{2k} - M^2 = 7 \quad \Rightarrow (2^k + M)(2^k - M) = 7.$$

$$\Rightarrow 2^k - M = 1, \quad 2^k + M = 7$$

$$\Rightarrow 2^k + 2^k - 1 = 7,$$

$$\text{or } 2^k = 4 \text{ i.e. } k = 2 \text{ and } n = 1.$$

Ref: M. Satyanarayan, Math Student 1968.

1.9. SOLUTION OF EQUATION IN PRIME NUMBERS :

We know many simple equations about which we do not know whether they have many solutions in prime numbers.

For example: The equation $x + y = z$. The solution of this equation in prime number x, y, z is equivalent to the question, whether there exists infinitely many pairs of twin primes, for, if p, q and r are prime numbers such that $p + q = r$, obviously the prime number p and q can not both be odd (because then their sum would be an even number > 2 and so composite). Therefore one of the numbers p and q , say q is even and so equal to 2. The numbers p and $r = p + 2$ would then be a pair of twin primes. If the number p and $r = p + 2$ are a pair of twin primes then the numbers $x = p, y = 2, z = p + 2$ are primes and give the solution of the equation $x + y = z$.

Consider the equation $2x \pm 1 = y$. We do not know they have infinitely many solutions. The solution of $2x + 1 = y$, $(x, y) = (2, 5), (3, 7), (5, 11), (11, 23)$ and for $2x - 1 = y$ are $(2, 3), (3, 5), (7, 13), (19, 37)$. Equations of the type $x + y = z + t$ and $x^2 + y^2 = z^2 + t^2$ have infinitely many solutions in distinct primes x, y, z and t .

1.10. MAGIC SQUARES :

A magic square consists of a series of integer arranged in a square so that the sum of the number in any row or column is always the same. Magic squares have been known since ancient times. The construction of magic squares is a favorite topic in recreational mathematics.

In early school days Ramanujan's attention was devoted in constructing magic squares.

The following are the examples of magic squares 3×3 with sum (i) $r = 15$ and

(ii) $r = 27$ where r is the sum of rows and columns.

6	1	8
7	5	3
2	9	4

$r = 15$

15	1	11
5	9	13
7	17	3

$r = 27$

Construction of magic squares :

Consider two sets of natural numbers. $S_1 = \{ A, B, C, \dots \}$, $S_2 = \{ P, Q, R, \dots \}$ each with n elements. Take the n^2 number in the direct sum $S_1 + S_2$ and arrange them in an $n \times n$ square so that each letter appears exactly once in each row, column and diagonal. Then we get a magic square.

Entry (i) : Let m_1 and m_2 denote the sum of the middle row and middle column respectively of a 3×3 square array of numbers. Let c_1 and c_2 denote the sums of the main diagonal and second diagonal, respectively. Let S denotes the sum of all nine elements of the square. Then if x denotes the centre element of the square

$$x = 1/3 (m_1 + m_2 + c_1 + c_2 - S).$$

It is clear that

$$m_1 + m_2 + c_1 + c_2 = S + 3x$$

as x is counted four times in the left side.

Entry (ii) : Suppose that the sum of each row and column is equal to r . Then if x denotes the centre element of the square then

$$x = 1/3 (c_1 + c_2 - r)$$

since by entry (i)

$$x = 1/3 (r + r + c_1 + c_2 - 3r) = 1/3 (c_1 + c_2 - r).$$

Note that if the square is magic, then entry (ii) implies that $x = r/3$ i.e. r is a multiple of 3.

Result : In a 3×3 magic square the elements in the middle row, middle column, and each diagonal are in arithmetic progression.

PROOF : In each case the second element or middle one is $r/3$. If a and b are the first and third elements, respectively then $a + r/3 + b = r$

$$\Rightarrow b - r/3 = r/3 - a$$

i.e. three numbers are in arithmetical progression.

Example 1 : $r = 15$ middle term $= 15/3 = 5$, $a + b = 10$.

The values of a and b are the pairs $(1, 9)$, $(2, 8)$, $(3, 7)$, $(4, 6)$.

6	1	8
7	5	3
2	9	4

$$r = 15$$

Example 2 : Construct magic square with (i) $r = 36$ and all elements even and (ii) $r = 63$ and all elements divisible by 3.

Solution: In the first case $x = 12$ and in the second case $x = 21$.

14	4	18
16	12	8
6	20	10

$$r = 36$$

24	9	30
27	21	15
12	33	18

$$r = 63$$

1.11. DISTRIBUTION OF PRIME NUMBERS :

We now introduce a function $\pi(x)$ which is a measure of distribution of primes amongst the natural number.

Definition : For each real number x , $\pi(x)$ denotes the number of primes that do not exceed x , i.e.

$$\pi(x) = \sum_{p \leq x} 1.$$

Example : $\pi(-1) = \pi(1) = 0, \pi(2) = \pi(5/2) = 1.$

THEOREM 31 (PRIME NUMBER THEOREM) :

The prime number theorem asserts that

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{(x / \log x)} = 1.$$

In Chapter 4 we will do elementary proof of this prime number theorem.

1.12. SOME MORE NUMBERS AND THEIR COMPUTER PROGRAMMING

AMICABLE NUMBERS OR FRIENDLY NUMBERS : Let m and n be two integers such that $\sigma(m) - m = n$ and $\sigma(n) - n = m$, then m and n are said to be amicable pair. Here $\sigma(m)$ denotes the sum of proper divisor of m .

Example : The smallest amicable number s are 220 and 284 because

$$\sigma(220) = 1+2+4+5+10+11+20+44+55+110 = 284$$

and $\sigma(284) = 1 + 2 + 4 + 71 + 142 = 220.$

THEOREM 32 : A pair of integers (m, n) is amicable if and only if

$$(9) \quad \sigma(m) = \sigma(n) = m + n.$$

PROOF : (i) Let $\sigma(m) = \sigma(n) = m + n$

$$\text{Then } \sigma(m) - m = n \text{ and } \sigma(n) - n = m.$$

Therefore (m, n) is an amicable pair.

(ii) Let (m, n) be an amicable pair then $\sigma(m) - m = n$ and $\sigma(n) - n = m$

Hence

$$\sigma(m) = m + n \text{ and } \sigma(n) = n + m. \text{ Hence proved.}$$

There are about 400 amicable pairs of numbers known, of which some are.

220 and	284 (the smallest pair)
1184	1210
2620	2924
5020	5564
6232	6368
10744	10856
12285	14595

17296	18416
63020	76084
66928	66992
67095	71145
69615	87633
79750	88730
9 363 584	9 437 056
111 448 537 712	118 853 793 424

Several methods are available for finding amicable pairs. One common method is to let

$$A = (3) (2^x) - 1$$

$$B = (3) (2^{x-1}) - 1$$

$$C = (9) (2^{2x-1}) - 1.$$

If x is greater than 1, and A , B , and C are all primes, then $2^x AB$ and $2^x C$ constitute an amicable pair of numbers. For example, if $x = 4$, then $A = 47$, $B = 23$, and $C = 1151$, which are all primes. Then

$$(2^4) (47) (23) = 17\ 296$$

and

$$(2^4) (1151) = 18\ 416.$$

The following is the BASIC program to produce the next pair of amicable numbers.

```

100      REM AMICABLE NUMBERS
110      FOR A = 1 TO 7000
120      LET S = 0
130      FOR D = 1 TO A/2
140      IF A/D <> INT (A/D) THEN 160
150      LET S = S+D
160      NEXT D
170      IF S <= A THEN 260
180      LET B = S
190      LET T = 0
200      FOR F = 1 TO B/2

```

```

210      IF B/F <> INT (B/F) THEN 230
220      LET T = T +F
230      NEXT F
240      IF T <.> a THEN 260
250      PRINT A; "AND";B; "ARE AMICABLE NUM-
        BER"
260      NEXT A
270      END

```

RUN

220 and 284 are amicable numbers.

1184 and 1210 are amicable numbers.

1.13. ARMSTRONG NUMBERS

One hundred fifty three is an interesting number because

$$153 = 1^3 + 5^3 + 3^3.$$

Numbers such as this are called Armstrong numbers. Any N digit number is an Armstrong number if the sum of the Nth power of the digits is equal to the original number.

The following program finds three –digit Armstrong numbers.

```

100      REM ARMSTRONG NUMBERS
110      FOR N = 100 TO 999
120      LET A = INT (N/100)
130      LET B = INT (N/10) – 10*A
140      LET C = N –100*A–10*B
150      IF N <> A3 + B3 + C3 THEN 190
160      PRINT "ARMSTRONG NUMBER";N
170      PRINT "EQUALS"; A3 + " + ";B3 + " + ";C3
180      PRINT
190      NEXT N
200      END

```

RUN

ARMSTRONG NUMBER 153

EQUALS $1 + 125 + 27$

ARMSTRONG NUMBER 370

EQUALS $27 + 343 + 0$

ARMSTRONG NUMBER 371

EQUALS $64 + 0 + 343$ **1.14. LUCKY NUMBERS**

A group of investigators working with Stanislaw M. Ulam at Los Alamos scientific laboratories have discovered what they call the lucky number determined by a sieving process. As with the sieve of Eratosthenes, we begin by writing down all the natural numbers, in order, limiting ourselves to the first hundred to illustrate the process. If we leave 1 and strike out every second number, we eliminate all the even numbers.

1	3	8	7	9
11	13	15	17	19
21	23	25	27	29
31	33	35	37	39
41	43	45	47	49
51	53	55	57	59
61	63	65	67	69
71	73	75	77	79
81	83	85	87	89
91	93	95	97	99

In Eratosthenes sieve we next struck out every multiple of 3 because 3 was the next surviving number. The rule here is different: strike out every third number among those remaining. That means that 5 goes, and 11. 17. 23, etc. All such numbers are crossed out by a single slant line. The next surviving number is 7, so we let that stand and cross out every seventh remaining one (19, 39, etc.) with two slant lines, to indicate what is happening. Then cross out every 9th, then every 13th, and so on. The slant lines indicate at what stage in the construction each number was eliminated.

1.15. ABUNDANT AND DEFICIENT NUMBERS

The number the sum of whose divisors is less than the number itself is called deficient, and a number exceeded by this sum is called abundant. As discussed in section 1.8, the number is perfect when the sum of the divisors of that number, excluding the number itself, equals the number in question.

For example,

$6 = 1 + 2 + 3$ and is perfect.

$12 < 1 + 2 + 3 + 4 + 6$ and is abundant.

$10 > 1 + 2 + 5$ and is deficient.

The following BASIC program factors a given number into its divisors and determines whether the number is abundant, deficient, or perfect.

```
100      REM ABUNDANT AND DEFICIENT NUM-
        BERS
110      PRINT "THIS PROGRAM WILL TAKE A
        NUMBER AND"
120      PRINT "COMPUTE THE SUM OF ITS DIVI-
        SORS"
130      PRINT
140      PRINT "TYPE THE NUMBER";
150      INPUT N
160      LET S = 0
170      PRINT "THE DIVISORS OF ";N;"ARE";
180      FOR X = 1 TO N-1
190      IF N/X <> INT 9N/X) THEN 220
200      LET S = S + X
210      PRINT X;
220      NEXT X
230      PRINT
240      IF S>N THEN 280
250      IF S<N THEN 300
260      PRINT N; "IS PERFECT"
270      GOTO 310
```

```

280 PRINT N; "IS ABUNDANT"
290 GOTO 310
300 PRINT N; "IS DEFICIENT"
310 PRINT
320 PRINT "TYPE 1 TO CONTINUE; 2 TO STOP";
330 INPUT Z
340 IF Z = 1 THEN 130
350 END

```

RUN

THIS PROGRAM WILL TAKE A NUMBER AND COMPUTE THE SUM OF ITS DIVISORS

TYPE THE NUMBER ? 12

THE DIVISORS OF 12 ARE 1 2 3 4 6 12 IS ABUNDANT

TYPE 1 TO CONTINUE, 2 TO STOP ? 1

The following is the BASIC program for computing prime Number generators less than 400:

```

10 REM PRIME NUMBER GENERATOR
12 DIM A[400]
15 PRINT "PRIME NUMBERS"
20 LET R=1
25 LET A[1]=2
30 LET P=1
35 FOR X = 3 TO 400 STEP 2
40 FOR Y = 1 TO R
45 IF INT (X/A[Y] * A{ Y} = X THEN 95
50 NEXT Y
55 LET R = R +1
60 LET S[R] = X
65 IF P>6 THEN 85
70 LET P = P+1

```

```

75      PRINT X;
80      GOTO 95
85      LET P=1
90      PRINT X
95      NEXT X

```

RUN

PRIME NUMBER

3	5	7	11	13	17	19
23	29	31	37	41	43	47
53	59	61	67	71	73	79
83	89	97	101	103	107	109
113	127	131	137	139	149	151
157	163	167	173	179	181	191
193	197	199	211	223	227	229
233	239	241	251	257	263	269
271	277	281	283	293	307	311
313	317	331	337	347	349	353
359	367	373	379	383	389	397

The following is the BASIC program that will determines whether a given number positive integer is a prime number

```

100      REM IS THE NUMBER PRIME ?
110      PRINT "WHAT IS THE NUMBER";
120      INPUT N
130      IF INT (N) = N THEN 160
140      PRINT N; "IS NOT AN INTEGER"
150      GOTO 250
160      IF N >= 2 THEN 190
170      PRINT N; "IS LESS THAN 2"
180      GOTO 250

```

```

190      FOR I = 2 TO SQR (N)
200      IF INT (N/I) = N/I THEN 240
210      NEXT I
220      PRINT N; "IS A PRIME NUMBER"
230      GOTO 250
240      PRINT N; "IS NOT A PRIME NUMBER"
250      PRINT
260      PRINT "TYPE 1 TO CONTINUE; 2 TO STOP";
270      INPUT C
280      IF C = 1 THEN 110
290      END

```

RUN

WHAT IS THE NUMBER ? 624

624 IS NOT A PRIME NUMBER

TYPE 1 TO CONTINUE; 2 TO STOP ? 1

WHAT IS THE NUMBER / 769

769 IS A PRIME NUMBER

TYPE 1 TO CONTINUE; 2 TO STOP ? 1

WHAT IS THE NUMBER ? 1

1 IS LESS THAN 2

TYPE 1 TO CONTINUE ; 2 TO STOP ? 1

WHATE IS THE NUMBER? 76,34

76, 34 IS NOT AN INTEGER

TYPE 1 TO CONTINUE; 2 TO STOP ? 1

WHAT IS THE NUMBER? 953

953 IS A PRIME NUMBER

TYPE 1 TO CONTINUE; 2 TO STOP ? 2

1.16. FIBONACCI NUMBERS

The sequence $u_1, u_2, u_3 \dots u_n$ in which $u_1 = 1, u_2 = 1, u_3 = 2$ and $(u_n = u_{n-1} + u_{n-2})$ for every $n \geq 2$ is called a Fibonacci sequence and it is termed as the Fibonacci number. The first few terms of the sequence are 1, 1, 2, 3, 5, 8, 13 ... as

$$u_4 = u_3 + u_2 = 2 + 1 = 3$$

$$u_5 = u_4 + u_3 = 3 + 2 = 5$$

$$u_6 = u_5 + u_4 = 5 + 3 = 8$$

and so on.

THEOREM 33 : For the Fibonacci sequence $\{u_n\}$, $\gcd(u_n, u_{n+1}) = 1$ for every $n \geq 1$.

PROOF : Let us suppose that the integer $d > 1$ divides both u_n and u_{n+1} . Then their difference $u_{n+1} - u_n = u_{n-1}$ will also be divisible by d . From this and from the relation $u_n u_{n-1} u_{n-2}$ it may be concluded that $d|u_{n-2}$. The same argument shows that $d|u_{n-3}, d|u_{n-4}$, and that $d|u_1$. But $u_1 = 1$. This contradicts our assumption that $d > 1$. hence $d = 1$.

The question is whether u_n is prime for n prime. The answer is no, because $u_{19} = 4181 = 37.113$.

THEOREM 34 : The greatest common divisor of two Fibonacci numbers is again a Fibonacci number, specially

$$\gcd(u_m, u_n) = u_d, \text{ where } d = \gcd(m, n).$$

PROOF : Assume that $m \geq n$. By Euclidean Algorithm we get

$$m = q_1 n + r_1, \quad 0 < r_1 < n$$

$$n = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2$$

.

.

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

$$\begin{aligned} \gcd(u_m, u_n) &= \gcd(u_{q_1 n + r_1}, u_n) \\ &= \gcd(u_{q_1 n - 1} u_r + u_{q_1 n} u_{r+1}, u_n) \\ &= \gcd(u_{q_1 n - 1} u_r, u_n). \end{aligned}$$

Since $\gcd(a+c, b) = \gcd(a, b)$,

$$\gcd(u_m, u_n) = \gcd(u_{r_1}, u_n)$$

$$\begin{aligned}
 &= \gcd(u_{r_1}, u_{r_2}) \\
 &= \dots = \gcd(u_{r_{n-1}}, u_{r_n}),
 \end{aligned}$$

Since $r_n | r_{n-1}$, we have $u_{r_n} | u_{r_{n-1}}$,

whence $\gcd(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$.

But r_n , being the last non zero remainder in the Euclidean Algorithm for m and n , is equal to $\gcd(m, n)$ we get

$$\gcd(u_m, u_n) = u_{\gcd(m, n)}.$$

Hence proved.

Corollary : In the Fibonacci sequence, $u_m | u_n$ if and only if $m | n$ for $m \geq 2$.

PROOF : If $u_m | u_n$, then $\gcd(u_m, u_n) = u_m$.

But $\gcd(u_m, u_n) = u_{\gcd(m, n)}$.

This implies that $\gcd(m, n) = m$. From which it follows that $m | n$.

Here we give a BASIC program that computes and prints 30 Fibonacci numbers.

```

100      REM FIBONACCI NUMBERS
110      DIM F [30]
120      PRINT "FIBONACCI NUMBERS"
130      PRINT
140      LET F[1] = 1
150      LET F[2] = 1
160      FOR N = 1 TO 28
170          LET F[N+2] = F[N+1] + F[N]
180      NEXT N
190      REM PRINT 30 FIBONACCI NUMBERS
200      FOR X = 1 TO 30
210          PRINT F[X]
220      NEXT X
230      END

```

RUN**FIBONACCI NUMBERS**

```

1
1
2
3
5
8
13
21
34
55
89
144
233
377
610
987
1597
2584
4181
6765
10946
17711
28657
46368
75025
121393
196418
317811
514229
832040

```

1.17. FIBONACCI NUMBERS AND PRIMES

The BASIC program in the last section produced the first thirty Fibonacci numbers. As you have observed, all of these Fibonacci numbers are integer quantities, and some are prime numbers.

Let us now consider the problem of generating Fibonacci numbers and identifying those that are primes. An outline of the program procedure is :

1. Set F1 and F2 to 1 (F1 is the first Fibonacci number (F_{n-2}) and F2 second Fibonacci number (F_{n-1}).
2. Print F1 and F2 identifying each as a prime number.
3. Perform the following calculations for $I = 3, 4, \dots, 25$.
 - (a) Calculate a value for F using the formula $F = F1 + F2$.
 - (b) Test to see if F is a prime number.
 - (c) If F is a prime, identify it as such.
 - (d) Update F1 and F2 in preparation for calculating a new Fibonacci number (assign the current value of F1 to F2, then assign the value of F to F1)

A BASIC program corresponding to the previous procedure follows :

```

100      REM FIBONACCI AND PRIME NUMBERS
110      PRINT "HOW MANY FIBONACCI NUM-
120      BERS";
130      INPUT N
140      PRINT
150      PRINT 'FIBONACCI AND PRIME NUM-
160      BERS"
170      PRINT
180      LET F1=1
190      LET F2=1
200      PRINT "I="; 1, "F="; 1, " (PRIME NUMBER)"
210      PRINT "I="; 2, "F="; 1, " (PRIME NUMBER)"
220      FOR I= 3 TO N
230      LET F= F1 +F2
240      FOR J=2 TO F-1
250      LET Q=F/J
260      LET Q1=INT (Q)
270      IF Q=Q1 THEN 300
      NEXT J

```

```

280      PRINT "I="; I, "F="; F; "(PRIME NUMBER)"
290      GOTO 310
300      PRINT "I="; I, "F="; F
310      LET F2=F1
320      LET F1=F
330      NEXT I
340      END

```

RUN

HOW MANY FIBONACCI NUMBERS?24

FIBONACCI AND PRIME NUMBERS

I = 1	F = 1	(PRIME NUMBER)
I = 2	F = 1	(PRIME NUMBER)
I = 3	F = 2	(PRIME NUMBER)
I = 4	F = 3	(PRIME NUMBER)
I = 5	F = 5	(PRIME NUMBER)
I = 6	F = 8	
I = 7	F = 13	(PRIME NUMBER)
I = 8	F = 21	
I = 9	F = 34	
I = 10	F = 55	
I = 11	F = 89	(PRIME NUMBER)
I = 12	F = 144	
I = 13	F = 233	(PRIME NUMBER)
I = 14	F = 377	
I = 15	F = 610	
I = 16	F = 987	
I = 17	F = 1597	(PRIME NUMBER)
I = 18	F = 2584	
I = 19	F = 4181	
I = 20	F = 6765	
I = 21	F = 10946	
I = 22	F = 17711	
I = 23	F = 28657	(PRIME NUMBER)
I = 24	F = 46368	

EXERCISES

1. Prove that if $(a, b) = 1$ then
 - (i) $(a^n, b^k) = 1$ for all $n \geq 1, k \geq 1$
 - (ii) $(a+b, a^2 - ab + b^2)$ is either 1 or 3.
 - (iii) $(a+b, a-b)$ is either 1 or 2.
2. Prove that $19 \mid 2^{6k+2} + 3$, for $k = 0, 1, 2, \dots$
3. Find all integers $n > 1$ such that $1^n + 2^n + \dots + (n-1)^n$ is divisible by n .
4. Prove that for positive integer n
 - (i) $n^2 \mid (n+1)^n - 1$
 - (ii) $(2^n - 1)^2 \mid 2(2^{2^n - 1})^n - 1$
5. Prove that for odd n , $n \mid 2^{n!} - 1$.
6. Prove that $(n, 2^{2^n} + 1) = 1$ for $n = 1, 2, \dots$
7. Find all primes which can be represented both as sums and as differences of two primes.
8. Find four solutions of the equation $p^2 + 1 = q^2 + r^2$ with primes p, q and r .
9. Find the least positive integer n for which $n^4 + (n+1)^4$ is composite.
10. Show that for $n > 1$ the number (i) $1/5 (2^{4n+2} + 1)$ is composite.
 (ii) $1/3 (2^{2^{n+1}} + 2^{2^n} + 1)$ is composite.
11. Find all numbers p such that all six number $p, p+2, p+6, p+8$ and $p+14$ are primes.
12. Prove that the Mersenne number M_{29} is composite.
13. Find all positive integer $n > 1$ for which $(n-1)! + 1 = n^2$.
14. Prove that
 - (a) $8 \mid 5^{2n} + 7$ [Hint: $5^{2(k+1)} + 7 = 5^2 (5^{2k} + 7) + (7 - 5^2 \cdot 7)$]
 - (b) $15 \mid 2^{4^n} - 1$
 - (c) $5 \mid 3^{3^{n+1}} + 2^{n+1}$
 - (d) $21 \mid 4^{n+1} + 5^{2n-1}$
 - (e) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.

15. Prove that $(2n)! / n! (n+1)!$ is an integer.
16. Prove that if $d \mid n$ then $2^d - 1 \mid 2^n - 1$.
17. Show that $a^n \mid b^n$ implies $a \mid b$.
18. Show that the Fermat number F_5 is divisible by 641.
19. For $n \geq 2$, show that the last digit of the Fermat number $F_n = 2^{2^n} + 1$ is 7.
20. If n is a perfect number prove that $\sum_{d \mid n} 1/d = 2$.
21. Prove that every even perfect number is a triangular number.
22. If m and n are amicable numbers prove that

$$\left(\sum_{d|m} 1/d\right)^{-1} + \left(\sum_{d|n} 1/d\right)^{-1} = 1$$



ARITHMETICAL FUNCTIONS

2.0. INTRODUCTION :

Number theory like many other branches of mathematics, concern with sequence of real or complex numbers.

DEFINITION : A real or complex valued function defined on the positive integer is called an arithmetical function or a number theoretic function. Symbolically we write arithmetical function as

$$f : \mathbb{Z}_+ \rightarrow \mathbb{R} (\mathbb{C}).$$

2.1. MOBIUS FUNCTION $\mu(n)$.

DEFINITION : The Mobius function μ is defined as follows:

$$\mu(1) = 1;$$

If $n > 1$, write $n = p_1^{a_1} \dots p_k^{a_k}$. Then

$$\mu(n) = (-1)^k \text{ if } a_1 = a_2 = \dots = a_k = 1$$

$$\mu(n) = 0 \text{ otherwise,}$$

i.e. $\mu(n) = 0$ if and only if n has a square factor > 1 . In other words

$$\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}.$$

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

Example 1. Find the value of $\mu(720)$.

Solution : $720 = 2^4 \times 3^2 \times 5$.

Hence $\mu(720) = 0$.

Example 2. Find $\sum_{k=1}^n \mu(k!)$.

$$\text{Solution : } \sum_{k=1}^n \mu(k!) = \mu(1) + \mu(2!) + \mu(3!) + \mu(4!) + \mu(5!) + \dots$$

$$= \mu(1) + \mu(2) + \mu(6) + \mu(24) + \dots$$

$$\sum_{k=1}^n \mu(k!) = 1 - 1 + 1 + 0 + 0 + \dots = 1.$$

Mobius function arises in many different places in number theory. We will study its most fundamental properties.

THEOREM 1 : If $n \geq 1$ we have

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where $I(n)$ is identity function.

PROOF : The formula is clearly true if $n = 1$. Assume, then, that $n > 1$ and

write $n = \prod_{t=1}^r p_t^{a_t}$. In the sum $\sum_{d|n} \mu(d)$ the only non zero terms come from $d = 1$ and from those divisor of n which are product of distinct primes. Thus

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \dots + \mu(p_r) + \mu(p_1 p_2) + \dots + \mu(p_{r-1} p_r)$$

$$+ \dots + \mu(p_1 p_2 \dots p_r)$$

$$\Rightarrow \sum_{d|n} \mu(d) = 1 + \binom{r}{2} (1) + \binom{r}{2} (-1)^2 + \dots + \binom{r}{r} (-1)^r$$

$$= (1-1)^r = 0.$$

DEFINITION : For each positive integer n ,

we denote $d(n)$ as

$$d(n) = \#\{k : k|n\} = \sum_{d|n} 1.$$

We also write $r(n)$ for $d(n)$.

$\sigma(n)$ = sum of the divisors of n ,

$$\sigma_k(n) = \sum_{d|n} d^k = \text{sum of the } k^{\text{th}} \text{ power of divisor of } n.$$

2.2. THE EULER TOTIENT FUNCTION $\Phi(n)$.

DEFINITION : If $n \geq 1$ the Euler totient $\phi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n ; thus

$$(1) \quad \phi(n) = \sum_{d|n} 1 = \text{Total number of integers less than } n \text{ and relatively prime to } n \quad (k, n) = 1.$$

TABLE 2

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

If $n = p$ (a prime) then $\phi(n) = \phi(p) = p-1$.

For example $\phi(8) = 4$, because 1, 3, 5, 7 are relatively prime to 4.

Now the question is how to find $\phi(n)$ when n is given in the standard form i.e.

$n = \prod_{i=1}^r p_i^{a_i}$. Like $\sum_{d|n} \mu(d)$ we will find the value of the summatory function of $\phi(n)$ i.e. $\sum_{d|n} \phi(d)$. The following theorem gives the answer to our question.

Before going to the theorem we will first define multiplicative function.

DEFINITION : An arithmetical function 'f' is called multiplicative if $f \equiv 0$ and if $f(mn) = f(m)f(n)$ for m, n ; such that $(m, n) = 1$.

A multiplicative function 'f' is called completely multiplicative if we also have

$$f(mn) = f(m)f(n) \text{ for all } m, n.$$

A function f which is completely multiplicative is multiplicative but the converse is not true.

Example1 : Let $f_\alpha(n) = n^\alpha$, where α is a fixed real or complex number.

f_α is completely multiplicative because $(mn)^\alpha = m^\alpha \cdot n^\alpha$ for all m, n . Hence $f_\alpha(n)$ is multiplicative.

Example 2 : The function $\mu(n)$ is multiplicative but not completely multiplicative. Consider first m, n such that $(m, n) = 1$. Either m or n has a square factor. Hence $\mu(mn) = \mu(m) \mu(n) = 0$. If neither has a square factor, write $m = p_1 p_2 \dots p_r$, $n = q_1 q_2 \dots q_k$, $\mu(mn) = (-1)^{r+k}$, $\mu(m) = (-1)^r$, $\mu(n) = (-1)^k$. Since $(-1)^{k+r} = (-1)^r (-1)^k$, we have $\mu(mn) = (-1)^{r+k} = (-1)^r (-1)^k = \mu(m) \mu(n)$. Hence μ is multiplicative. But $\mu(n)$ is not completely multiplicative since $\mu(8) = 0$, $8 = 2^3$, $\mu(2) = -1$, $\mu(2^3) = (-1)(-1)(-1) = -1$. $\mu(8) \neq \mu(2) \mu(2) \mu(2)$.

Example 3 : Find $\phi(720)$.

$$\begin{aligned} 720 &= 2^4 \times 3^2 \times 5, \quad \phi(720) = 720 \times (1 - 1/2)(1 - 1/3)(1 - 1/5) \\ &= 12 \times 2 \times 4 = 96. \end{aligned}$$

THEOREM 2 : If p is a prime and $k > 0$, then $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

PROOF : There are p^{k-1} integer between 1 and p^k i. e.

$p, 2p, 3p, \dots, (p^{k-1})p$ which are divisible by p . The set $\{1, 2, \dots, p^k\}$ contains exactly $p^k - p^{k-1}$ integer which are relatively prime to p^k and so, by definition of Euler's ϕ function $\phi(p^k) = p^k - p^{k-1}$.

For example

$$\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4.$$

$$\phi(27) = \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18.$$

LEMMA : $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, a, b, c are integers.

PROOF : Let $d = \gcd(a, b)$ then by definition of \gcd $d|a$ and $d|b$ whence $d|a$ and $d|bc$. This implies $\gcd(a, bc) \geq d$ which forces $d = 1$. Similarly for $(a, c) = 1$.

Only if part: Let $\gcd(a, b) = 1 = \gcd(a, c)$ and assume that $\gcd(a, bc) = d_1 > 1$. Since $d_1 | bc$, it follows $p | bc$; p is a prime divisor of d_1 . Hence $p | b$ or $p | c$. If $p | b$ then $\gcd(a, b) \geq p$, a contradiction. Similar argument follows for $\gcd(a, c)$.

Thus $d_1 = 1$.

Example 4 : The function $\phi(n)$ is a multiplicative function but not completely multiplicative function. $\phi(n)$ is not completely multiplicative follows from the fact that

$$\phi(4) = 2, \quad \phi(2) = 1, \quad \phi(4) \neq \phi(2) \phi(2).$$

Multiplicity of $\phi(n)$ will be proved in the next chapter on congruence.

THEOREM 3 : If the integer $n > 1$ has the prime factorization $n = \prod_{i=1}^r p_i^{a_i}$

$$\text{then } \varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

PROOF : If $n = p^k$, there are $p^k - 1$ positive numbers less than p^k , of which $p^{k-1} - 1$ are multiples of p and the remainder prime to p .

Hence

$$\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k (1 - 1/p)$$

and the general value of $\varphi(n)$ follow from the multiplicity of $\varphi(n)$.

$$\text{Since } n = \prod_{i=1}^r p_i^{a_i}, \quad \varphi(n) = \prod_{i=1}^r \varphi(p_i^{a_i})$$

$$= \prod_{i=1}^r p_i^{a_i} (1 - 1/p_i)$$

$$= \prod_{i=1}^r p_i^{a_i} \prod_{i=1}^r (1 - 1/p_i)$$

$$= n \prod_{i=1}^r (1 - 1/p_i) = n \prod_{p|n} (1 - 1/p).$$

The right hand side product is independent of prime power of n .

THEOREM 4 : $\sum_{d|n} \varphi(d) = n$.

PROOF : If $n = \prod_{p|n} p^k$, then the divisor of n are the numbers $d = \prod_{p|n} p^k$, where $0 \leq k \leq k$ for each p ; and

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{p, k^1} \prod \varphi(p^{k^1}) \\ &= \prod_p \{1 + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k)\} \text{ by the multiplicative property of } \varphi(n). \end{aligned}$$

$$\text{But } 1 + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k)$$

$$= 1 + (p-1) + p(p-1) + \dots + p^{k-1}(p-1)$$

$$= p^k.$$

So that

$$\sum_{d|n} \varphi(d) = \prod_{p|n} p^k = n.$$

We can prove theorem 4 without using multiplicative property.

Second method of proof of theorem 4 : Let 'S' denote the set $\{1, 2, \dots, n\}$. We distribute the integers of S into disjoint set as follows: For each divisor d of n, let

$$A(d) = \{k: (k, n) = d, 1 \leq k \leq n\}.$$

$$\bigcup_d A(d) = S.$$

If f(d) denotes the number of integer in A(d) we have

$$\sum_{d|n} f(d) = n.$$

But $(k, n) = d$ if and only if $(k/d, n/d) = 1$,

and $0 < k \leq n$ if and only if $0 < k/d \leq n/d$.

Put $q = k/d$ then $0 < q \leq n/d$. There is one-to-one correspondence between the elements in A(d) and those integers q such that $(q, n/d) = 1$. The number of such q is $\varphi(n/d)$. Hence $f(d) = \varphi(n/d)$. We have

$$\sum_{d|n} \varphi(n/d) = n.$$

This implies $\sum_{d|n} \varphi(d) = n$, because if d runs through divisor of n so does n/d.

This completes the proof.

RELATION BETWEEN $\Phi(n)$ AND $\mu(n)$.

THEOREM 5 : If $n \geq 1$, we have $\varphi(n) = \sum_{d|n} \mu(d) n/d$.

$$\text{PROOF : } \varphi(n) = \sum_{\substack{k=1 \\ (n,k)=1}}^n 1 = \sum_{k=1}^n [1/(n,k)]$$

where $[x]$ is the greatest integer function.

By Theorem 1.

$$\varphi(n) = \sum_{k=1}^n \sum_{d|(n,k)} \mu(d) = \sum_{d|n} \sum_{d|k} \mu(d).$$

For a fixed divisor d of n we sum over all those k in the range $1 \leq k \leq n$ which are multiples of d .

Taking $k = qd$, $1 \leq k < n$ if and only if $1 \leq q \leq n/d$. Hence

$$\begin{aligned}\varphi(n) &= \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 \\ &= \sum_{d|n} \mu(d) n/d.\end{aligned}$$

Remark. Theorem 3 can be deduced from theorem 5 by using the fact that

$$\begin{aligned}\prod_{p|n} (1 - 1/p) &= \prod_{i=1}^r (1 - 1/p_i) \\ &= 1 - \sum 1/p_i + \sum 1/p_i p_j - \dots + (-1)^r / (p_1 + p_2 - \dots + p_r) \\ &= \sum_{d|n} \mu(d)/d.\end{aligned}$$

$$\text{Hence } \varphi(n) = \sum_{d|n} \mu(d) n/d = n \prod_{p|n} (1 - 1/p).$$

THEOREM 6 : If $d = (m, n)$, then $\varphi(mn) = \varphi(m) \varphi(n) (d/\varphi(d))$.

PROOF : $\varphi(n)/n = \prod_{p|n} (1 - 1/p)$, $\varphi(m)/m = \prod_{p|m} (1 - 1/p)$.

Since every prime divisor of mn is either a divisor of m or n , and those primes which divide both m and n also divide (m, n) , we have

$$\begin{aligned}\varphi(mn)/mn &= \prod_{p|mn} (1 - 1/p) = \frac{\prod_{p|m} (1 - 1/p) \prod_{p|n} (1 - 1/p)}{\prod_{p|(m,n)} (1 - 1/p)} \\ &= \frac{\varphi(m)/m \cdot \varphi(n)/n}{\varphi(d)/d} \\ &\Rightarrow \varphi(mn) = \varphi(m) \varphi(n) (d/\varphi(d)).\end{aligned}$$

Corollary : $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m, n) = 1$. It is trivial by putting $d = 1$ in Theorem 6.

THEOREM 7 : $\varphi(n)$ is even for $n \geq 3$. If n has r distinct odd prime factors then $2^r | \varphi(n)$.

PROOF : If $n = 2^r$, $r \geq 2$ $\varphi(n) = \varphi(2^r) = 2^r - 2^{r-1}$ implies that $\varphi(n)$ is even for $n \geq 3$. If n has at least one odd prime factor we write

$$\phi(n) = n \prod_{p|n} (p-1/p)$$

$$= \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1)$$

$$= k \prod_{p|n} (p-1),$$

where $k = n / \prod_{p|n} p$ is an integer and since p is odd, $p-1$ is even. If n has r distinct odd prime factor then $2^r | \phi(n)$.

Remark : All $\phi(n)$ are even. Only odd $\phi(n)$ are for $n = 2$ and $n = 1$.

Example : Evaluate $\phi(350)$.

$$\text{As } 350 = 2 \times 5^2 \times 7$$

$$\phi(350) = \phi(2) \phi(5^2) \phi(7) = 1 \times (5^2 - 5) \cdot 6 = 120.$$

THEOREM 8 : Let m and n be integer both greater than 1 and every prime divisor of n is a prime divisor of m . Then

$$(i) \quad \phi(mn) = n \phi(m)$$

$$(ii) \quad \phi(n^2) = n \phi(n) \text{ for all } n \geq 1.$$

PROOF : (i) By hypothesis m and n can be written as

$$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$$

$$\text{and } m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} p_{k+1}^{s_{k+1}} \dots p_t^{s_t},$$

p_i being prime, r_i, s_i integers each ≥ 1 and $t \geq k$.

$$\phi(mn) = \phi(p_1^{s_1+r_1} p_2^{s_2+r_2} \dots p_k^{s_k+r_k} p_{k+1}^{s_{k+1}} \dots p_t^{s_t})$$

$$= \phi(p_1^{s_1+r_1}) \dots \phi(p_k^{s_k+r_k}) \dots \phi(p_t^{s_t})$$

$$= (p_1^{s_1+r_1} - p_1^{s_1+r_1-1}) (p_2^{s_2+r_2} - p_2^{s_2+r_2-1}) \dots$$

$$\phi(p_{k+1}^{s_{k+1}}) \dots \phi(p_t^{s_t})$$

$$= (p_1^{r_1} \dots p_k^{r_k} (p_1^{s_1} - p_1^{s_1-1}) (p_2^{s_2} - p_2^{s_2-1}) \dots$$

$$\phi(p_{k+1}^{s_{k+1}}) \dots \phi(p_t^{s_t})$$

$$= m \cdot \phi(p_1^{s_1}) \dots \phi(p_t^{s_t})$$

$$= m \phi(n).$$

Putting $m = n$ we get (ii)

But if the same prime divides both m and n then $n \phi(m) = m \phi(n)$ is not always true. For example taking $m = 6, n = 8, 8 \cdot \phi(6) \neq 6 \cdot \phi(8)$

Example : If $(m, n) = 1$ then $(\phi(m), \phi(n)) = 1$ is not always true. For example take $m = 6, n = 7, (6, 7) = 1$. But $\phi(m) = 2, \phi(n) = 6, (\phi(m), \phi(n)) > 1$.

THEOREM 9 : For $n > 1$, the sum of the positive integer is less than n and relatively prime to n is $\frac{1}{2} n\phi(n)$.

PROOF : Let $a_1 a_2 \dots a_{\phi(n)}$ be the positive integers less than n and relatively prime to n . Now since $\gcd(a, n) = 1$ if and only if $\gcd(n-a, n) = 1$, we have

$$\begin{aligned} a_1 + a_2 + \dots + a_{\phi(n)} &= (n-a_1) + (n-a_2) + \dots + (n-a_{\phi(n)}) \\ &= \phi(n) n - (a_1 + a_2 + \dots + a_{\phi(n)}) \end{aligned}$$

$$\text{Hence, } 2(a_1 + a_2 + \dots + a_{\phi(n)}) = \phi(n) n$$

$$\Rightarrow a_1 + a_2 + \dots + a_{\phi(n)} = n \phi(n) / 2.$$

Example : $\sum_{\substack{1 \leq k \leq 20 \\ \gcd(k, 20)=1}} k = 1 + 3 + 7 + 11 + 13 + 17 + 19.$

$$= 80 = 20\phi(20) / 2.$$

$$\phi(20) = \phi(2^2, 5) = \phi(2^2) \phi(5) = 2 \times 4 = 8.$$

THEOREM 10 : Let f and F be number theoretic function such that

$$F(n) = \sum_{d|n} f(d).$$

Then, for any positive integer N ,

$$\sum_{n=1}^N F(n) = \sum_{k=1}^N f(k) [N/k],$$

PROOF : We note that

$$(1) \quad \sum_{n=1}^N F(n) = \sum_{k=1}^N \sum_{d|n} f(d)$$

For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if k is a divisor of n . There are exactly $[N/k]$ number of terms among $1, 2, \dots, N$ which are divisible by k . They are $k, 2k, 3k, \dots, [N/k]k$. Thus for each k such that $1 \leq k \leq N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $[N/k]$ different positive integer less than or equal to N . We may write the double sum in (1) as

$$\sum_{n=1}^N \sum_{d|n} f(d) = \sum_{k=1}^N f(k) [N/k].$$

Example 1 : $\sum_{d=1}^n \phi(d) [n/d] = n(n+1)/2$ for any positive integer n .

Solution : By Theorem 9,

$$\begin{aligned}\sum_{d=1}^n \varphi(d)[n/d] &= \sum_{k=1}^n \sum_{d|k} \varphi(d) \\ &= \sum_{k=1}^n k = 1 + 2 + \dots + n = n(n+1)/2.\end{aligned}$$

Example 2 : Prove that $n/\varphi(n) = \sum_{d|n} \mu^2(d) / \varphi(d)$.

Solution : If $n = p_1 p_2 \dots p_r$ (We consider the product of distinct primes only because $\mu(n) = 0$, if n contains a square).

Again $\mu^2(n) / \varphi(n)$ is multiplicative.

Let
$$G(n) = \sum_{d|n} \mu^2(d) / \varphi(d)$$

If
$$n = \sum_{i=1}^r p_i^{a_i}$$

then
$$G(n) = \sum_{i=1}^r G(p_i^{a_i})$$

$$\begin{aligned}&= (1 + 1/\varphi(p_1))(1 + 1/\varphi(p_2)) \dots (1 + 1/\varphi(p_r)) \\ &= (p_1/p_1 - 1)(p_2/p_2 - 1) \dots (p_r/p_r - 1) \\ &= 1/(1 - 1/p_1) 1/(1 - 1/p_2) \dots 1/(1 - 1/p_r) \\ &= n/\varphi(n).\end{aligned}$$

Example 3 : Find all integers n such that

(i) $\varphi(n) = \varphi(2n)$

(ii) $\varphi(n) = n/2$

(iii) $\varphi(n) = 12$

Solution : Proof of (i) $\varphi(n) = \varphi(2n)$ holds for $n = 1, 3, 5, 7, \dots$

(ii) $\varphi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 1$.

If
$$n = 2^k, \quad \varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1} = n/2$$

If
$$n = 2^k N, \quad N \text{ is odd then}$$

$$\varphi(n) = \varphi(2^k N) = 2^{k-1} N / 2$$

$$\Rightarrow \varphi(2^k) \varphi(N) = 2^{k-1} N.$$

$$\Rightarrow 2^{k-1} \varphi(N) = 2^{k-1} N.$$

$$\Rightarrow N = 1.$$

(iii) $12 = 3 \times 4$. Suppose $n = st$, $\varphi(st) = \varphi(s) \varphi(t)$

To show that $\varphi(s) = 3$, $\varphi(t) = 4$.

There is no s for which $\varphi(s) = 3$.

$$12 = 2 \times 6, \quad \varphi(3) = 2, \quad \varphi(7) = 6.$$

$$\varphi(4) = 2$$

$$12 = 12 \times 1 \quad \varphi(6) = 2$$

$$\varphi(13) = 12, \varphi(2) = 1, \quad \varphi(1) = 1$$

The number are $n = 13, 21, 26, 28, 42$.

Example 4 : Find all solutions of (i) $\varphi(n) = 24$ and (ii) $\varphi(n) = 16$

Solution : (i) $\varphi(n) = 24$

(ii) $\varphi(n) = 16$

We factorize $24 = 3 \times 8$

$$= 2 \times 12$$

$$= 6 \times 4$$

In the first case there is no value of n for which $\varphi(n)$ is 3 hence we discard the first factor. Consider the second and third factors.

$$\varphi(3) = 2 \quad \varphi(13) = 12 \quad \varphi(5) = 4 \quad \varphi(12) = 4$$

$$\varphi(4) = 2 \quad \varphi(7) = 6 \quad \varphi(9) = 6$$

$$\varphi(6) = 2 \quad \varphi(10) = 4 \quad \varphi(8) = 4$$

So the integer n for which

$\varphi(n) = 24$ is given by 35, 39, 45, 52, 56, 70, 72, 78, 84, 90.

Verification : Since $(3,13) = 1$

$$\varphi(39) = \varphi(3 \times 13) = \varphi(3) \times \varphi(13) = 2 \times 12 = 24$$

$$(4,13) = 1 \Rightarrow \varphi(52) = \varphi(4 \times 13) = \varphi(4) \varphi(13) = 2 \times 12 = 24$$

$$(6,13) = 1 \Rightarrow \varphi(78) = \varphi(6 \times 13) = \varphi(6) \varphi(13) = 2 \times 12 = 24$$

$$(5,7) = 1 \Rightarrow \varphi(35) = \varphi(5 \times 7) = \varphi(5) \varphi(7) = 4 \times 6 = 24$$

$$(7,10) = 1 \Rightarrow \varphi(70) = \varphi(7 \times 10) = \varphi(7) \varphi(10) = 6 \times 4 = 24.$$

(ii) $\varphi(n) = 16 = 2 \times 8 = 16 \times 1 = 4 \times 4$

$$\varphi(3) = 2 \quad \varphi(5) = 4 \quad \varphi(17) = 16$$

$$\varphi(4) = 2 \quad \varphi(8) = 4 \quad \varphi(2) = 1$$

$$\varphi(6) = 2 \quad \varphi(10) = 4$$

$$\varphi(1) = 1$$

$$\varphi(16) = 8 \quad \varphi(15) = 8$$

So the solution of $\phi(n) = 16$ are

$$n = 17, 32, 34, 40, 48, 60.$$

Example 5 : There are infinitely many integers n for which (i) $10 \mid \phi(n)$ and (ii) $\phi(n)$ is a perfect square.

Solution : (i) $\phi(11^k) = 11^k - 11^{k-1} = 11^{k-1} \cdot 10$

Hence $10 \mid \phi(n)$ where $n = 11^k, k = 1, 2, 3, \dots$

(ii) If $n = 2^{2k+1}, k = 1, 2, 3, 4, \dots$

Then $\phi(2^{2k+1}) = 2^{2k+1} - 2^{2k} = 2^{2k}(2-1) = 2^{2k} = (2^k)^2$

Hence for $n = 2^{2k+1}, k = 1, 2, 3, 4, \dots$ $\phi(n)$ is a perfect square.

2.3. ARITHMETICAL FUNCTION $d(n)$ AND $\sigma(n)$.

DEFINITION 1 : The number of positive divisors of n is called as divisor function and is denoted as $d(n)$.

$$d(n) = \sum_{d|n} 1.$$

DEFINITIONS 2 : The sum of the positive divisors of n is denoted as $\sigma(n)$. Symbolically we write

$$\sigma(n) = \sum_{d|n} d.$$

We define $\sigma_\alpha(n)$ as

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha \quad \alpha \geq 0$$

If $\alpha = 0, \sigma_0(n) = d(n)$.

If $\alpha = 1, \sigma_1(n) = \sigma(n)$.

Example : $n = 6, d(n) = 4,$

$$\sigma(n) = 1 + 2 + 3 + 6 = 12$$

If n is a prime p then $d(n) = 2$, and $\sigma(n) = 1 + p$, To find formula for $\sigma(n)$ when n is in the standard form.

THEOREM 11 : If $n = p_1^{a_1} \dots p_r^{a_r}$, then

$$d(n) = (a_1+1)(a_2+1) \dots (a_r+1) \text{ and}$$

$$\sigma(n) = \prod_{i=1}^r \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

PROOF : If $n = p^a$ the divisors are

$1, p, p^2, \dots, p^a$ i.e. there are $a+1$ number of divisors of p^a .

Hence $d(p^a) = a + 1$

and $\sigma(n) = \sigma(p^a) = 1 + p + p^2 + \dots + p^a = p^{a+1} - 1 / (p - 1)$.

Assume that the theorem is true whenever n has k or fewer distinct prime factors.

Let $n = n' p^a$ where n' has k distinct prime factor and p , which is prime not a factor of n'

If $n' = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

then $d(n') = (a_1 + 1)(a_2 + 1) \dots (a_k + 1)$

and $\sigma(n') = \prod_{i=1}^r \frac{p_i^{a_i+1} - 1}{p_i - 1}$.

Let d_1, d_2, \dots, d_s denote the $d(n')$ divisor of n' . Then the divisor of n are $d_1, d_2, \dots, d_s, p d_1, p d_2 \dots p d_s, p^2 d_1, p^2 d_2, \dots, p^a d_1, p^a d_2, \dots, p^a d_s$.

Thus

$$\begin{aligned} d(n) &= d(n')(a+1) \\ &= (a_1 + 1)(a_2 + 1) \dots (a_k + 1)(a + 1) \end{aligned}$$

and similarly

$$\begin{aligned} \sigma(n) &= \sigma(n') + p \sigma(n') + \dots + p^a \sigma(n') \\ &= \sigma(n') (1 + p + \dots + p^a) \\ &= \sigma(n') \left(\frac{p^{a+1} - 1}{p - 1} \right) \end{aligned}$$

$$= \sum_{i=1}^k \left(\frac{p_i^{a_i+1} - 1}{p_i - 1} \right) (p^{a+1} - 1 / p - 1).$$

Our theorem follows by mathematical induction.

Corollary 1 : If $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$

then $d(n) = d(p_1^{a_1}) d(p_2^{a_2}) \dots d(p_s^{a_s})$

$$\sigma(n) = \sigma(p_1^{a_1}) \sigma(p_2^{a_2}) \dots \sigma(p_s^{a_s})$$

That is $d(n)$ and $\sigma(n)$ are multiplicative functions.

Example 1 : $d(100) = d(2^2 \times 5^2) = 3 \times 3 = 9$.

$$\sigma(100) = ((2^3 - 1)/(2 - 1)) ((5^3 - 1)/(5 - 1)) = 7 \times 31 = 217.$$

Example 2 : $\prod_{d|n} d = n^{d(n)/2}$.

Solution : If $n = p^\alpha$, divisors of n are $1, p, p^2, \dots, p^\alpha$

Hence $\prod_{d|p^\alpha} d = 1, p, p^2, \dots, p^\alpha = p^{\alpha(\alpha+1)/2} = (p^\alpha)^{(\alpha+1)/2} = (p^\alpha)^{d(p^\alpha)/2}$

In this case $\prod_{d|n} d = n^{d(n)/2}$.

If $n = \prod_{p|n} p^\alpha$, $d(n) = \prod_{p|n} d(p^\alpha)$.

Hence $\prod_{d|n} d = \prod_{p|n} \left(\prod_{d|p^\alpha} d \right) = \left\{ \prod_{p|n} (p^\alpha)^{d(p^\alpha)/2} \right\} = n^{d(n)/2}$.

Second solution : $d | n \Rightarrow n = d d'$

$\Rightarrow d' | n$ and $d' = n/d$. The divisor d of n are in pairs $(d, n/d)$

$\Rightarrow (\text{product of all divisor of } n)^2 = \left(\prod_{d|n} (d) \right)^2 = n^{d(n)}$

$\Rightarrow \prod_{d|n} (d) = n^{d(n)/2}$.

2.4. GENERALIZED EULER'S TOTIENT FUNCTION.

We generalize Euler's totient function $\phi(n)$ to $\phi(x, n)$ as follow:

Let x be a positive real number and for all n let $\phi(x, n)$ = the number of integers y such that $1 \leq y \leq x$ and $(y, n) = 1$.

Thus $\phi(n, n) = \phi(n)$. For all x and n ,

$$\phi(x, n) = \sum_{d|n} \mu(d) [x/d].$$

Also we can extend $\phi(n)$ to $\phi(*, k)$ as follows $\phi(n, k)$ = the number of integer x such that $1 \leq x \leq n$ and $(x, n) = (n + k - x, n) = 1$

$$\phi(*, n) = \phi.$$

If $(m, n) = 1$, then

$$\phi(mn, k) = \phi(m, k) \phi(n, k)$$

i. e. $\phi(*, k)$ is a multiplicative function.

$$\text{THEOREM 12 : } \phi(n, k) = n \prod_{p|n} \left(1 - \frac{\varepsilon(p)}{p} \right).$$

$$\text{where } \varepsilon(p) = \begin{cases} 1 & \text{if } p|k \\ 2 & \text{if } p \nmid k. \end{cases}$$

The proof is difficult.

2.5. LIOUVILLE'S FUNCTION $\lambda(n)$.

We define another arithmetical function $\lambda(n)$ called as Liouville's function as follows .

DEFINITION : We have $\lambda(1) = 1$ and if $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ we define

$$\lambda(n) = (-1)^{a_1 + a_2 + a_3 + \dots + a_k}$$

$\lambda(n)$ is completely multiplicative since if $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$;

$$\begin{aligned} m &= q_1^{b_1} q_2^{b_2} \dots q_s^{b_s} \\ \lambda(nm) &= (-1)^{a_1 + a_2 + \dots + a_k + b_1 + b_2 + \dots + b_s} \\ &= (-1)^{a_1 + a_2 + \dots + a_k} (-1)^{b_1 + b_2 + \dots + b_s} \\ &= \lambda(n) \lambda(m) \text{ for all } m, n. \end{aligned}$$

THEOREM 13 : For every $n \geq 1$ we have

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise.} \end{cases}$$

PROOF : Let $g(n) = \sum_{d|n} \lambda(d)$. Then g is multiplicative, so to determine $g(n)$ we need only to compute $g(p^a)$ for prime powers. We have

$$\begin{aligned} g(p^a) &= \sum_{d|p^a} \lambda(d) = 1 + \lambda(p) + \lambda(p^2) + \dots + \lambda(p^a) \\ &= 1 - 1 + 1 - \dots + (-1)^a \\ &= \begin{cases} 0 & \text{if } a \text{ is odd} \\ 1 & \text{if } a \text{ is even} \end{cases} \end{aligned}$$

Hence if $n = \prod_{i=1}^r p_i^{a_i}$ we have

$$g(n) = \prod_{i=1}^r g(p_i^{a_i}). \text{ If any exponent } a_i \text{ is odd then } g(p_i^{a_i}) = 0 \text{ so } g(n) = 0.$$

If all the exponents a_i are even then $g(p_i^{a_i}) = 1$ for all i and $g(n) = 1$. This proves that $g(n) = 1$ if n is a square and $g(n) = 0$ otherwise.

Hence proved.

2.6. VON-MANGOLDT FUNCTION

We define Mangoldt function $\Lambda(n)$ as follows :

DEFINITION : For every integer $n \geq 1$ we define

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^m \text{ for some prime } p \text{ and some } m \geq 1 \\ 0 & \text{otherwise.} \end{cases}$$

TABLE 1 : VALUES OF $\Lambda(N)$

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

We note that $\Lambda(2) = \Lambda(2^k)$

i.e. $\Lambda(p) = \Lambda(p^k)$, p is a prime and $k > 1$. It is important to find the summatory function $\sum_{d|n} \Lambda(d)$.

THEOREM 14 : If $n \geq 1$ we have

$$(2) \quad \sum_{d|n} \Lambda(d) = \log n.$$

PROOF : The theorem is trivial when $n = 1$ because $\Lambda(1) = 0 = \log 1$. Assume

$$n > 1 \text{ and write } n = \prod_{i=1}^r p_i^{a_i}.$$

Taking logarithm of both sides we have

$$\log n = \sum_{i=1}^r a_i \log p_i.$$

Consider the L.H.S $\sum_{d|n} \Lambda(d)$.

The only non-zero terms in the sum came from those divisors d of the form p_i^m for $m = 1, 2, \dots, a_i$ and $i = 1, 2, \dots, r$.

Hence

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{i=1}^r \sum_{m=1}^{a_i} \Lambda(p_i^m) \\ &= \sum_{i=1}^r \sum_{m=1}^{a_i} \log p_i = \sum_{i=1}^r a_i \log p_i = \log n.\end{aligned}$$

This proves (2).

THEOREM 15 : If $n \geq 1$ we have

$$\Lambda(n) = \sum_{d|n} \mu(d) \log n/d = - \sum_{d|n} \mu(d) \log d$$

PROOF :

$$\begin{aligned}\Lambda(n) &= \sum_{d|n} \mu(d) \log n/d = \sum_{d|n} \mu(d) (\log n - \log d) \\ &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= - \sum_{d|n} \mu(d) \log d.\end{aligned}$$

by theorem 1, as the first term is zero.

2.7. AVERAGES OF ARITHMETICAL FUNCTION.

We have observed that some arithmetical function behave most irregularly for large value of n . So we consider the average or mean of such arithmetical functions.

$$\overline{f(n)} = 1/n \sum_{k=1}^n f(k).$$

$\overline{f(n)}$ behave more regularly than $f(n)$. Also we have

$$(3) \quad \lim_{n \rightarrow \infty} d(n) / \log n = 1.$$

We call the average order of $d(n)$ is $\log n$. To study the average of an arbitrary function $f(n)$ we need a knowledge of its partial sums $\sum_{k=1}^n f(k)$.

DEFINITION : If $g(x) > 0$ for all $x \geq a$,

we write $f(x) = O(g(x))$

i.e. there exists a constant $M > 0$ such that $|f(x)| \leq M g(x)$ for all $x \geq a$.

DEFINITION : If $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$.

We say that $f(x)$ is asymptotic to $g(x)$ as $x \rightarrow \infty$,

and we write $f(x) \sim g(x)$ as $x \rightarrow \infty$.

The key theorem for all the theorems on the averages of arithmetical function is the following Euler's summation formula.

THEOREM 16 : If f has a continuous derivative f' on the interval $[y, x]$, where $0 < y < x$, then

$$(4) \sum_{y < n \leq x} f(n) = \int_y^x f(t) dt + \int_y^x (t - [t]) f'(t) dt + f(x)([x] - x) - f(y)([y] - y).$$

PROOF : Let $m = [y]$, $k = [x]$. For integer n and $n-1$ in $[y, x]$ we have

$$\begin{aligned} \int_{n-1}^n [t] f'(t) dt &= \int_{n-1}^n (n-1) f'(t) dt \\ &= (n-1) \{f(n) - f(n-1)\} \\ &= \{n f(n) - (n-1) f(n-1)\} - f(n). \end{aligned}$$

Summing from $n = m + 1$ to $n = k$ we have

$$\begin{aligned} \sum_{n=m+1}^k \int_{n-1}^n [t] f'(t) dt &= \sum_{n=m+1}^k \{n f(n) - (n-1) f(n-1)\} - \sum_{n=m+1}^k f(n) \\ \Rightarrow \int_m^k [t] f'(t) dt &= k f(k) - m f(m) - \sum_{y < n \leq x} f(n) \\ \Rightarrow \sum_{y < n \leq x} f(n) &= - \int_m^k [t] f'(t) dt + k f(k) - m f(m) \\ &\quad + k f(x) - m f(y) - k f(x) + m f(y) \end{aligned}$$

$$(5) \quad \Rightarrow \quad \sum_{y < n \leq x} f(n) = - \int_y^x [t] f'(t) dt + kf(x) - mf(y)$$

Again

$$(6) \quad \int_y^x f(t) dt = xf(x) - yf(y) - \int_y^x tf'(t) dt$$

Subtracting (6) from (5) we have

$$\begin{aligned} \sum_{y < n \leq x} f(n) - \int_y^x f(t) dt &= - \int_y^x [t] f'(t) dt + kf(x) - mf(y) \\ &\quad - xf(x) + yf(y) + \int_y^x tf'(t) dt = \int_y^x (t - [t]) f'(t) dt + f(x) ([x] - x) \\ &\quad - f(y) ([y] - y) \\ \Rightarrow \quad \sum_{y < n \leq x} f(n) &= \int_y^x f(t) dt + \int_y^x (t - [t]) f'(t) dt + f(x) ([x] - x) \\ &\quad - f(y) ([y] - y). \end{aligned}$$

THEOREM 17 : If $x \geq 1$ we have

$$(a) \quad \sum_{n \leq x} 1/n = \log x + C + O(1/x), \text{ } C \text{ is a constant.}$$

$$(b) \quad \sum_{n \geq x} 1/n^s = O(x^{1-s}) \text{ if } s > 1.$$

$$(c) \quad \sum_{n \geq x} n^\alpha = x^{\alpha+1}/\alpha+1 + O(x^\alpha) \text{ if } \alpha \geq 0.$$

PROOF : To prove (a)

take $f(t) = 1/t$ in theorem 16 to obtain

$$\sum_{n \leq x} 1/n = \int_1^x dt/t - \int_1^x t - [t]/t^2 dt + 1 - (x - [x])/x$$

$$\begin{aligned}
 &= \log x - \int_1^x t - [t]/t^2 dt + 1 + O(1/x) \\
 &= \log x + 1 - \int_1^\infty t - [t]/t^2 dt + \int_1^\infty t - [t]/t^2 dt + O(1/x)
 \end{aligned}$$

Now

$$0 \leq \int_x^\infty t - [t]/t^2 dt \leq \int_x^\infty 1/t^2 dt = 1/x$$

So we get

$$\begin{aligned}
 \sum_{n \leq x} 1/n &= \log x + 1 - \int_1^\infty t - [t]/t^2 dt + O(1/x) \\
 &= \log x + C + O(1/x),
 \end{aligned}$$

$$\text{if } C = 1 - \int_1^\infty t - [t]/t^2 dt$$

$$(b) \sum_{n > x} 1/n^s = \sum_{n=1}^\infty 1/n^s - \sum_{n \leq x} 1/n^s = O(x^{1-s}) \text{ if } s > 1.$$

(c) Taking $f(t) = t^\alpha$ we obtain

$$\begin{aligned}
 \sum_{n \leq x} n^\alpha &= \int_1^x t^\alpha dt + \alpha \int_1^x t^{\alpha-1} (t - [t]) dt + 1 - (x - [x]) x^\alpha \\
 &= x^{\alpha+1} / \alpha + 1 - 1/\alpha + 1 + O(\alpha) \int_1^x t^{\alpha-1} dt + O(x^\alpha) \\
 &= x^{\alpha+1} / \alpha + 1 + O(x^\alpha).
 \end{aligned}$$

THEOREM 18 : For all $x \geq 1$ we have

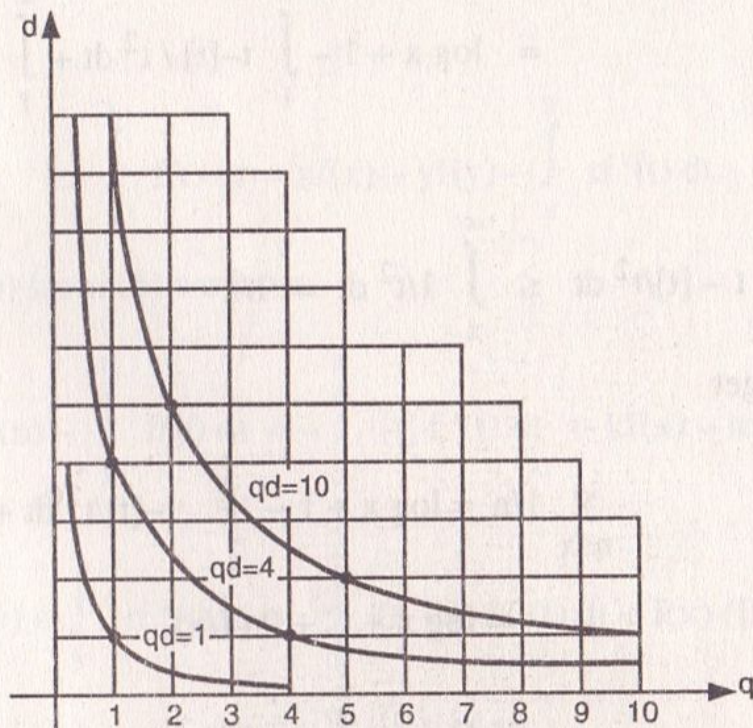
$$\sum_{n \leq x} d(n) = x \log x + O(x).$$

i.e. $\sum_{n \leq x} d(n) \sim x \log x$ as $x \rightarrow \infty$.

PROOF : Since $d(n) = \sum_{d|n} 1$ we have

$$(7) \sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{\substack{q, d \\ qd \leq x}} 1 = \sum_{\substack{q, d \\ qd \leq x}} 1.$$

(Since $d|n$ we write $n = qd$ with $qd \leq x$)



The sum is extended over certain lattice point in the qd -plane (by lattice point we mean points with integer coordinates). The lattice points with $qd = n$ lie on a hyperbola, so the sum in (7) counts the number of lattice points which lie on the hyperbola corresponding to $n = 1, 2, \dots, [x]$. For each fixed $d \leq x$ we can count first those lattice points on the horizontal line segment $1 \leq q \leq x/d$, and then sum over all $d \leq x$. Then (7) becomes.

$$(8) \sum_{n \leq x} d(n) = \sum_{d \leq x} \sum_{d \leq x/d} 1 \\ = \sum_{d \leq x} [x/d + O(1)]$$

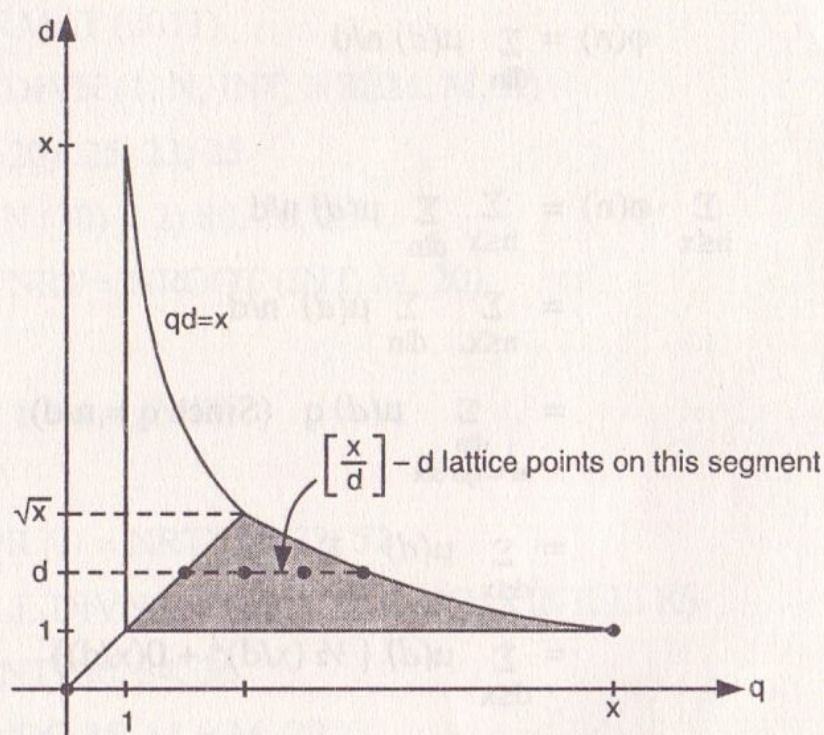
(by (c) of Theorem 15)

$$= x \sum_{d \leq x} 1/d + O(x) \\ = x \{ \log x + C + O(1/x) \} + O(x) \quad (C \text{ is a constant}) \\ = x \log x + O(x).$$

That is $\sum_{n \leq x} d(n) \sim x \log x$ as $x \rightarrow \infty$.

THEOREM 19 : For $x \geq 1$

$$(9) \sum_{n \leq x} d(n) = x \log x + (2C-1)x + O(\sqrt{x}).$$

PROOF :

The total number of lattice points in the region about the line $q = d$ is equal to twice the number below the $q = d$ plus the number on the bisecting line segments. Thus

$$\begin{aligned}\sum_{n \leq x} d(n) &= 2 \sum_{n \leq \sqrt{x}} \{ [x/d] - d \} + [\sqrt{x}] \\ &= 2 \sum_{d \leq \sqrt{x}} \{ x/d + O(1) - d \} + O(\sqrt{x})\end{aligned}$$

$$\begin{aligned}(\text{Since } [x/d] &= x/d + \{x/d\}) \\ &= x/d + O(1))\end{aligned}$$

$$\begin{aligned}&= 2x \sum_{d \leq \sqrt{x}} 1/d + O(1) \sum_{d \leq \sqrt{x}} 1 - 2 \sum_{d \leq \sqrt{x}} d + O(\sqrt{x}) \\ &= 2x \{ \log \sqrt{x} + C + O(1/\sqrt{x}) \} + O(\sqrt{x}) - 2 \{ x/2 + O(\sqrt{x}) \} + O(\sqrt{x}) \\ &= x \log x + (2C-1)x + O(\sqrt{x}).\end{aligned}$$

This completes the proof of the theorem 19.

This formula (9) is due to Dirichlet and is an improvement over the formula (8).

THEOREM 20 : For $x > 1$ we have

$$(10) \quad \sum_{n \leq x} \varphi(n) = 3/\pi^2 x + O(x \log x).$$

So the average order of $\varphi(n)$ is $3n/\pi^2$

PROOF : We know

$$\varphi(n) = \sum_{d|n} \mu(d) n/d$$

Hence

$$\begin{aligned} \sum_{n \leq x} \varphi(n) &= \sum_{n \leq x} \sum_{d|n} \mu(d) n/d \\ &= \sum_{n \leq x} \sum_{d|n} \mu(d) n/d \\ &= \sum_{\substack{d|n \\ n=qd \leq x}} \mu(d) q \quad (\text{Since } q = n/d) \\ &= \sum_{d \leq x} \mu(d) \sum_{q \leq x/d} q \\ &= \sum_{d \leq x} \mu(d) \left\{ \frac{1}{2} (x/d)^2 + O(x/d) \right\} \\ (11) \quad &= \frac{1}{2} x^2 \sum_{d \leq x} \mu(d)/d^2 + O\left(x \sum_{d \leq x} 1/d\right) \end{aligned}$$

But

$$(12) \quad \sum_{d \leq x} \mu(d)/d^2 = \sum_{d=1}^{\infty} \mu(d)/d^2 - \sum_{d > x} \mu(d)/d^2 = 6/\pi^2 + O\left(\frac{1}{x}\right)$$

Putting (12) in (11) we obtain

$$\begin{aligned} \sum_{n \leq x} \varphi(n) &= \frac{1}{2} x^2 \left\{ 6/\pi^2 + O(1/x) \right\} + O(x \log x) \\ &= (3/\pi^2) x^2 + O(x \log x). \end{aligned}$$

This completes the proof .

2.8. COMPUTER PROGRAMMING FOR DETERMINING PRIME FACTORIZATION OF N AND VALUE OF PHIN ($\Phi(N)$), TAUN($\tau(N)=d(N)$) AND SIGMA (N) ($\sigma(N)$)

C FOR ANY INTEGER N IN THE RANGE 2

C THROUGH 1, 073, 938, 400 THIS

C PROGRAM DETERMINES THE PRIME FACTORIZATION OF N AND VALUES

C PHI (N), TAU (N), AND SIGMA (N)

DIMENSION NPR (3512), N FAC (10), NBR (10), N (20), INT (20), NQ (20) DIMENSION NPHI (10), NSIG (10) LIMIT = 3512

10 FORMAT (1615)

```

15 READ (2.20) (NCI), 1 = 1, 20)
20 FORMAT (2011)
CALL DIVN (1, N, INT, NREM, M, K)
IF (M=20) 25, 23, 25
23 IF (N (20) = 2) 80, 70, 25
25   NRT = NROOT (INT, M. 20)
J = 0
DO 50 1 = 1, LIMIT.
NF = 0
IF (NPR (I) = NRT) 32, 32, 52
32 (ALL DIVN (NPR (1), INT, NQ, KINT, L. K)
IF (KINT) 36, 34, 36
34   DO 35. 11 = M, 20
35   INT (11) = NQ (11)
NF = NF + 1
GO TO 32
36 IF (NF) 50, 50, 38,
38 J = J + 1
NFAC (J) = NPR (I)
NBR (J) = NF
NRT = NROOT (INT, 1, 20)
50 CONTINUE
51 IF (J) 70, 70, 60
60 WRITE (3, 61) (N (K), K = M, 20)
61 FORMAT (1 HO, 1011)
WRITE (3, 62) (NFAC (K)),
N B R (K) , K = 1, J
62 FORMAT (1H +, 10 X, 3H = , 9 (15, 1H (j 12, 1H) ))
CALL PTS (NFAC, J, NBP, NPH 1, NTAU, N SIG, NDP, NDS, O)
IF (L = 20), 66, 64, 66
64 IF (INT (20) = 1 ) 75, 75, 66

```

```

66 WRITE (3, 67) (INT (K), K = L, 20)
67 FORMAT (1H, 15 X, 1011)
K = 1
GO TO 73
70 WRITE (3, 71) (N (K), K = M, 20)
71 FORMAT ( 1 HO, 1011)
WRITE (3, 72)
72 FORMAT ( 1H +, 13 X, BTHIS PRIME)
K = -1
73 DO 74 IA = 1, 10
74 NFAC (IA) = INT (IA + 10)
NBR (1) = 1
CALL PTS (NFAC, 1 , NBR, NPHI, NTAU, NSIG, NDP, NDS, K )
75 WRITE (3, 76) (N PHI (K), K = NDP, 10)
76 FORMAT ( 1H, 5X, 6HTAV=, 15)
77 WRITE (3, 78) (NSIG (K), K = NDS, 10)
78 FORMAT (1H, 5X, 8HSIGMA = , 1011)
GO TO 15
80 CALL EXIT
END

```

RESULT

```

405769 = 7 (4) 13 (2)
PH 1 = 321048
TAU = 15
SIGMA = 46448640
13123110 = 2 (1) 3 (1) 5 (1) 7 (2) 11 (1) 13 (1) 19 (1) 23 (1)
PH 1 = 228 0969
TAU = 256
SIGMA = 46448640
18061 IS PRIME
PH 1 = 18060

```

$$\text{TAU} = 2$$

$$\text{SIGMA} = 18062$$

$$62742247 \text{ IS PRIME}$$

$$\text{PH1} = 62742246$$

$$\text{TAU} = 2$$

$$\text{SIGMA} = 62742248$$

$$62742255 = 3 (1) 5 (1) 599 (1) 6983 (1)$$

$$\text{PH1} = 33401888$$

$$\text{TAU} = 16$$

$$\text{SIGMA} = 100569600$$

$$N = 62742267 = 3(2) 7(1) 995909(1)$$

$$= 35852688$$

$$\text{TAU} = 12$$

$$\text{SIGMA} = 103574640$$

EXERCISES

- Evaluate : (i) $\phi(5186)$, (ii) $\phi(56800)$,
(iii) $\phi(7208)$, (iv) $\phi(640412)$, (v) $\phi(628)$,
(vi) $\phi(1001)$.
- If for $n > 1$, $\phi(n) \mid n-1$, prove that n is square free.
- Prove that $\mu(n) \mu(n+1) \mu(n+2) \mu(n+3) = 0$ for each positive integer n .
- If $n = \prod_{i=1}^r p_i^{a_i}$ prove that
 - $\sum_{d \mid n} \mu(d) d(k) = (-1)^r$.
 - $\sum_{d \mid n} \mu(d) \sigma(d) = (-1)^r p_1 p_2 \dots p_r$.
 - $\sum_{d \mid n} |\mu(d)| = 2^r$.
- Prove that $\sum_{d \mid n} 1/d = \sigma(n) / n$ for each integer $n \geq 1$.
- Prove that
 - $d(n)$ is odd if and only if n is a perfect square,

- (ii) $\sigma(n)$ is odd if and only if n is a perfect square or twice a perfect square.
7. Prove that $\sum_{k|n} (d(k))^3 = \left(\sum_{k|n} d(k) \right)^2$ for each integer $n \geq 1$.
 8. For any integer n , show that
 - (i) $\sum_{k|n} \sigma(k) = \sum_{k|n} (n/k) d(k)$ and
 - (ii) $\sum_{k|n} (n/k) \sigma(k) = \sum_{k|n} k d(k)$.
 9. For $k \geq 2$ show that
 - (i) If $2^k - 1$ is prime then $2^{k-1} (2^k - 1)$ satisfies the equation $\sigma(n) = 2n$.
 - (ii) If $2^k - 3$ is prime, then $n = 2^{k-1} (2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.
 10. Prove that:
 - (i) If n is an even integer then $\phi(2n) = 2 \phi(n)$
 - (ii) $\phi(3n) = 3\phi(n)$ if and only if $3|n$.
 - (iii) $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $2p-1$ are both odd prime.
 11. Prove that if $a|b$ then $\phi(a)|\phi(b)$.
 12. Prove that if n is a perfect number i. e. $\sigma(n) = 2n$ then $\sum_{d|n} 1/d = 2$.
 13. Prove that $\sum_{d|n} \mu(d) \phi(d) = \prod_{p|n} (2-p)$.
 14. Prove that $\prod_{d^2|n} \mu(d) = \mu^2(n)$.
 15. Show that $\phi(n) = n-1$ if and only if n is prime.
 16. Find all values of n for which $\phi(n) = 6$.



CONGRUENCES

3.1. DEFINITION AND BASIC PROPERTIES OF CONGRUENCES.

Gauss in his great work, the "*Disquisitiones Arithmeticae*" in 1801 introduced a remarkable notation and basic facts which simplifies many problems concerning divisibility of integers. In doing so he created a new branch of number theory called the theory of congruences which is discussed in this chapter.

DEFINITION : Given integers a, b, m with $m > 0$, we say that a is congruent to b modulo m , and we write

$$(1) \quad a \equiv b \pmod{m},$$

if m divides the difference $a - b$. The number m is called the modulus of the congruence .

In other words, the congruence (1) is equivalent to the divisibility relation

$$m \mid a - b.$$

In particular, $a \equiv 0 \pmod{m} \Leftrightarrow m \mid a$.

Hence $a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m}$.

We write $a \not\equiv b \pmod{m}$ if $m \nmid (a-b)$

and we say a and b are incongruent modulo m .

Congruences are of great practical importance in everyday life. For example today is 'Thursday' is a congruence property (modulo 7) of the number of days that have passed since some fixed date. Lecture lists or railway guides are table of congruences, in the lecture list the relevant moduli are 365, 7 and 24.

Example 1 : Suppose that a lecture is given on every alternate date (including sundays), and that the first lecture occurs on a Monday. When will a

lecture first fall on a Tuesday ? If this lecture is $(x+1)^{\text{th}}$ then $2x \equiv 1 \pmod{7}$ and we find by trial the least positive solution is $x = 4$.

Thus the fifth lecture will fall on a Tuesday and this will be the first that will do so.

Example 2 : Consider $x^2 \equiv 1 \pmod{8}$.

We can find by trial the solutions which are $x \equiv 1, 3, 5, 7 \pmod{8}$.

The congruence is also called as modular arithmetic. So modular arithmetic or congruence is finite. Many interesting problems on divisibility, remainder which when divided by an integer can be carried out with the help of congruence.

BASIC PROPERTIES OF CONGRUENCES

THEOREM 1 : Congruence ' \equiv ' is an equivalence relation. That is we have

- (a) $a \equiv a \pmod{m}$ (Reflexivity).
- (b) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (Symmetry)
- (c) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$
 $\Rightarrow a \equiv c \pmod{m}$ (Transitivity).

PROOF :

- (a) follows since $m \mid a - a = 0$.
- (b) follow from the fact that if $m \mid (a-b)$ then $m \mid (b-a)$
- (c) If $m \mid (a-b)$ and $m \mid (b-c)$ then $m \mid (a-b) + (b-c) = a-c$ (divisibility property).

THEOREM 2 : If $a \equiv b \pmod{m}$ and $\alpha \equiv \beta \pmod{m}$, then we have

- (a) $ax + \alpha y \equiv bx + \beta y \pmod{m}$ for all integers x and y
- (b) $a\alpha \equiv b\beta \pmod{m}$
- (c) $a^n \equiv b^n \pmod{m}$ for every positive integer n .
- (d) $f(a) \equiv f(b) \pmod{m}$ for every polynomial f with integer coefficients.
- (e) If $d \mid m$, $d \mid a$ then $d \mid b$.
- (f) $(a, m) = (b, m)$.
- (g) If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ where $(m, n) = 1$ then $a \equiv b \pmod{mn}$.

PROOF : (a) Since $m \mid (a-b)$ and $m \mid (\alpha-\beta)$ we have

$$m \mid x(a-b) + y(\alpha - \beta) = (ax + \alpha y) - (bx + \beta y).$$

(b) $a\alpha - b\beta = \alpha(a-b) + b(\alpha-\beta) \equiv 0 \pmod{m}$ by (a).

(c) Take $\alpha = a$ and $\beta = b$ in (b) and using induction on n we get (c).

(d) Using (c) and induction on the degree of f we get (d).

(e) Assume that $d > 0$. If $d \mid m$ then $a \equiv b \pmod{m}$.

But if $d \mid a$ then $a \equiv 0 \pmod{m}$ so $b \equiv 0 \pmod{m}$.

(f) Let $d_1 = (a, m)$ and $d_2 = (b, m)$. Then $d_1 \mid m$ and $d_1 \mid a$ so $d_1 \mid b$; hence $d_1 \mid d_2$. Similarly $d_2 \mid m$, $d_2 \mid m$ implied $d_2 \mid a$; hence $d_2 \mid d_1$.

Therefore $d_1 = d_2$ i.e. $(a, m) = (b, m)$.

(g) Since both m and n divide $a - b$ so does their product mn since $(m, n) = 1$. Hence proved..

Example 3 : An integer is divisible by 9 if and only if, the sum of its digits in its decimal representation is divisible by 9.

$$\text{Suppose } n = a_0 + 10a_1 + 10^2a_2 + \dots + 10^ka_k.$$

$$\begin{aligned} 10 &\equiv 1 \pmod{9} \quad 10^2 \equiv 1 \dots\dots\dots 10^k \equiv 1 \pmod{9} \quad 10^ka_k \\ &\equiv 1 \pmod{9} \end{aligned}$$

$$\text{for } k = 0, 1, 2, \dots, k$$

So

$$n \equiv a_0 + a_1 + a_2 + \dots + a_k \pmod{9}$$

Since $3 \mid 9$ an integer is divisible by 3 if and only if, the sum of its digit in its decimal representation is divisible by 3.

Example 4 : An integer is divisible by 4 if and only if the difference between the sum of digits in the odd places and the sum of digits in the even place is divisible by 11.

Suppose

$$n = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \dots + 10^ka_k$$

$$1 \equiv 1 \pmod{11} \Rightarrow a_0 \equiv a_0 \pmod{11}$$

$$10 \equiv -1 \pmod{11} \Rightarrow 10a_1 \equiv -a_1 \pmod{11}$$

$$10^2 \equiv 1 \pmod{11} \Rightarrow 10^2a_2 \equiv a_2 \pmod{11}$$

$$10^3 \equiv -1 \pmod{11} \Rightarrow 10^3a_3 \equiv -a_3 \pmod{11}$$

$$10^k \equiv +1 \pmod{11} \text{ if } k \text{ is even}$$

$$10^k \equiv -1 \pmod{11} \text{ if } k \text{ is odd.}$$

Thus $a_0 + 10a_1 + \dots + 10^k a_k \equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + \dots) \pmod{11}$

So n is divisible by 11 if

$$(a_0 + a_2 + \dots + a_{k-1}) - (a_1 + a_3 + \dots + a_k) \equiv 0 \pmod{11}.$$

Example 5 : We have shown in the Chapter I that F_5 is composite and divisible by 641.

Here with the help of congruence we will show it.

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1.$$

Now $2^2 \equiv 4, 2^4 \equiv 16, 2^8 \equiv 256, 2^{16} \equiv 65,536 \equiv 154 \pmod{641}.$

$$\text{So } 2^{32} \equiv (154)^2 = 23,716$$

$$\equiv 640 \pmod{641}$$

$$\equiv -1 \pmod{641}.$$

Therefore, $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$, so F_5 is composite.

Example 6 : What is the remainder when 5^{48} is divided by 12 ?

$$\begin{aligned} \text{Now, } 5^{48} &= (5^2)^{24} = (25)^{24} \equiv (1)^{24} \pmod{12} \\ &\equiv 1 \pmod{12}. \end{aligned}$$

Hence the remainder is 1.

Example 7 : Find the remainder when $1! + 2! + 3! + \dots + 200!$ is divided by 4.

$$1! + 2! + 3! + \dots + 200!$$

$$\equiv 1! + 2! + 3! \pmod{4} \text{ (since } k! \text{ is divisible by 4)}$$

$$\equiv 1 + 2 + 6 \equiv 1 \pmod{4} \text{ for } k \geq 4$$

Hence the remainder is 1.

Example 8 : Determine the remainder when 2^{36} is divided by 11.

$$\text{Solution : } 2^{11} \equiv 2 \pmod{11}$$

$$\Rightarrow (2^{11})^3 \equiv 2^3 \pmod{11}$$

$$2^{36} = 2^{33} \cdot 2^3$$

$$\equiv 2^3 \cdot 2^3 \pmod{11}$$

$$\equiv 64 \pmod{11} \equiv 9 \pmod{11}.$$

Hence the remainder is 9.

Exercise

1. Find the last two digits of the number 9^{9^9} .

Example 9 : Find the remainder when 2^{14} is divided by 17.

$$2^4 \equiv -1 \pmod{17} \Rightarrow 2^8 \equiv 1 \pmod{17}. \text{ Again } 2^6$$

$$= 64 \equiv 13 \pmod{17}$$

$$2^{14} = 2^8 \cdot 2^6 \equiv 64 \pmod{17} \equiv 13 \pmod{17}.$$

Congruence is like equality '=' in arithmetic. All the properties of addition, subtraction, multiplication are true for congruence as shown in theorem 2. But the division is not always true for congruence. For example

$$18 \equiv 8 \pmod{10} \Rightarrow 9 \not\equiv 4 \pmod{10} \text{ since } 10 \nmid (9-4) = 5$$

Example 10 : (a) Find the remainder when 2^{50} and 41^{65} are divided by 7.

(b) What is the remainder when the sum $1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5$ is divisible by 4?

Solution :

$$(a) \quad 2^3 \equiv 1 \pmod{7}, 2^2 \equiv 4 \pmod{7}$$

$$\text{These two imply } 2^5 \equiv 4 \pmod{7}, 2^{10} \equiv 4^2 \pmod{7} \equiv 2 \pmod{7}$$

$$\text{Hence } 2^{50} \equiv 2^5 \pmod{7} \equiv 4 \pmod{7}.$$

Hence the remainder is 4.

$$\text{Again } 41 \equiv (-1) \pmod{7} \Rightarrow (41)^{65} \equiv (-1)^{65} \pmod{7}$$

$$\equiv -1 \pmod{7}$$

$$\equiv 6 \pmod{7}.$$

The remainder is 6.

(b)

$$1^5 \equiv 1 \pmod{4} \Rightarrow 1^5 \equiv 1 \pmod{4} \quad 2^5 \equiv 0 \pmod{4}$$

$$3^5 \equiv -1 \pmod{4} \Rightarrow 3^5 \equiv (-1)^5 \pmod{4}$$

$$4^5 \equiv 0 \pmod{4} \dots 100 \equiv 0 \pmod{4}.$$

All the even powers are divisible by 4. The odd terms are congruent to either 1 or -1 modulo 4. Hence

$$1^5 + 2^5 + 3^5 + \dots + 99^5 + 100^5 \equiv 1^5 + (-1)^5 \pmod{4}$$

$$\equiv (1-1) \pmod{4}$$

$$\equiv 0 \pmod{4}.$$

Example 11 : $2222^{5555} + 5555^{2222}$ is divisible by 7.

We know

$$2222 \equiv 3 \pmod{7}$$

and

$$5555 \equiv 4 \pmod{7}.$$

$$5555 \equiv 5 \pmod{6}$$

$$2222 \equiv 2 \pmod{6}.$$

$$\begin{aligned} \text{Thus } 2222^{5555} + 5555^{2222} &\equiv 3^5 + 4^2 \\ &\equiv 12 + 2 \pmod{7} \\ &\equiv 0 \pmod{7}. \end{aligned}$$

Example 12 : Using congruence we can also show that

$$(i) 13 \mid 3^{n+2} + 4^{2n+1} \quad (ii) 43 \mid 6^{n+2} + 7^{2n+1}$$

Example 13 : Show that $41 \mid 2^{20} - 1$.

$$\begin{aligned} 2^5 &\equiv -9 \pmod{41} \Rightarrow (2^5)^4 \equiv (-9)^4 \pmod{41} \\ \Rightarrow 2^{20} &\equiv 81.81 \pmod{41} \text{ But } 81 \equiv -1 \pmod{41} . \end{aligned}$$

$$\text{Hence } 2^{20} - 1 \equiv 81.81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}.$$

In the following theorem we will show when this cancellation law is true for congruence. We show that a common factor can be cancelled if the modulus is also divisible by this factor.

THEOREM 3 : If $c > 0$ then $a \equiv b \pmod{m}$ if and only if

$$ac \equiv bc \pmod{mc}.$$

PROOF : We have $m \mid (b-a)$ if and only if $mc \mid c(b-a)$, i. e. $ac \equiv bc \pmod{mc}$

THEOREM 4 : (Cancellation law) If $ac \equiv bc \pmod{m}$ and if $d = (m, c)$, then

$$a \equiv b \pmod{m/d}$$

If $d = 1$ we get

$$a \equiv b \pmod{m}.$$

That is, we can cancel the common factor which is relatively prime to the modulus .

PROOF : Since $ac \equiv bc \pmod{m}$ we have

$$m \mid c(a-b) \Rightarrow m/d \mid c/d(a-b)$$

But $(m, c) = d \Rightarrow (m/d, c/d) = 1$. Hence by Euclid's lemma $m/d \mid (a-b)$ i.e. $a \equiv b \pmod{m/d}$. Hence proved .

3.2. RESIDUE CLASSES AND COMPLETE RESIDUE SYSTEM

DEFINITION : Consider a fixed modulus $m > 0$. We denote by \hat{a} the set of integers x such that $x \equiv a \pmod{m}$

i.e. $\hat{a} = \{x: x \text{ is an integer and } x \equiv a \pmod{m}\}$.

We call \hat{a} the residue class a modulo m . Thus \hat{a} consists of all integers of the form $a + mk$, $k = 0, \pm 1, \pm 2 \dots$. The following property is satisfied by the residue classes.

Example : $\hat{0}, \hat{1}, \hat{2}, \dots, \hat{9}$ are the residue classes modulo 10.

THEOREM 5 : For a given modulus m we have

- (a) $\hat{a} = \hat{b}$, if and only if, $a \equiv b \pmod{m}$
- (b) Two integer x and y are in the same residue class if and only if $x \equiv y \pmod{m}$
- (c) The m residue classes $\hat{1}, \hat{2}, \dots, \hat{m}$ are disjoint and their union is the set of all integers.

PROOF :

- (a) $\hat{a} = \hat{b} \Leftrightarrow x \equiv a \pmod{m} = b \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$
- (b) $x \equiv y \pmod{m} \Leftrightarrow \hat{x} = \hat{y}$ by (a). Hence two integers x and y are in the same residue classes.
- (c) To prove (c) we note that the numbers $0, 1, 2, \dots, m-1$ are incongruent module m . Hence the residue classes $\hat{0}, \hat{1} \dots \widehat{m-1}$ are disjoint. But every integer x must be in exactly one of these classes because $x = qm + r$ where $0 \leq r < m$, so $x \equiv r \pmod{m}$ and hence $x \in \hat{r}$. Since $\hat{0} = \hat{m}$ this proves (c).

DEFINITION : A set of m representative one from each of the residue classes $\hat{1}, \hat{2}, \dots, \hat{m}$ is called a COMPLETE RESIDUE SYSTEM modulo m . We write in short as CRS modulo m .

Example : (i) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is a CRS (mod 11).

(ii) $\{1, m+2, 2m+3, 3m+4, \dots, m^2\}$

$\{0, 1, 2, \dots, m-1\}, \{1, 2, 3, \dots, m\}$ are the set m integers, incogruent module m are CRS modulo m .

3.3. REDUCED RESIDUE SYSTEM AND FERMAT'S THEOREM

DEFINITION: The set of $\phi(m)$ integers incongruent modulo m , each of which is relatively prime to m is a REDUCED RESIDUE SYSTEM modulo m . We write in short RRS modulo m .

Example 1 : If $m = 8$ then

$\{ 1, 3, 5, 7 \}$ form the RRS modulo 8.

Also $\{ 9, 11, 13, 15 \}$ form RRS modulo 8.

THEOREM 6 : Assume $(k, m) = 1$. If $\{ a_1, a_2, \dots, a_m \}$ is complete residue system modulo m , so is $\{ k a_1, k a_2, \dots, k a_m \}$.

PROOF : We will show that the elements of the set $\{ k a_1, k a_2, \dots, k a_m \}$ are distinct and mutually incongruent modulo m . Suppose they are not, then $k a_i \equiv k a_j \pmod{m}$ since $(k, m) = 1$ by cancellation law $a_i \equiv a_j \pmod{m}$ which is not true by the hypothesis that $\{ a_1, a_2, \dots, a_m \}$ is a CRS mod m . Therefore two elements in the set $\{ k a_1, k a_2, \dots, k a_m \}$ are mutually incongruent modulo m . Since there are m elements in this set it forms a CRS modulo m .

THEOREM 7 : Assume $(k, m) = 1$. If $\{ a_1, a_2, \dots, a_{\phi(m)} \}$ is a reduced residue system modulo m , then $\{ k a_1, k a_2, \dots, k a_{\phi(m)} \}$ is also a reduced residue system modulo m .

PROOF : Since $\{ a_1, a_2, \dots, a_{\phi(m)} \}$ is a RRS modulo m by definition $(a_i, m) = 1$ for $i = 1, 2, \dots, \phi(m)$. It is given that $(k, m) = 1$. These two imply $(k a_i, m) = 1$. That is each $k a_i$, $i = 1, 2, \dots$ is relatively prime to m .

So there are $\phi(m)$ in number.

Now $k a_i \equiv k a_j \pmod{m}$, $(k, m) = 1$

$\Rightarrow a_i \equiv a_j \pmod{m}$ which is false since $\{ a_1, a_2, \dots, a_{\phi(m)} \}$ runs through a RRS modulo m . Hence $\{ k a_1, k a_2, \dots, k a_{\phi(m)} \}$ also forms a RRS modulo m .

THEOREM 8 : (Fermat's Little Theorem)

For any integer a and any prime p we have

$$a^p \equiv a \pmod{p}.$$

This will follow from the generalised version called Euler Fermat theorem.

THEOREM 9 : (Euler Fermat-theorem)

Assume $(a, m) = 1$. Then we have $a^{\phi(m)} \equiv 1 \pmod{m}$.

PROOF : Let $\{ b_1, b_2, \dots, b_{\phi(m)} \}$ be a reduced residue system modulo m . Then $\{ a b_1, a b_2, \dots, a b_{\phi(m)} \}$ is also a reduced residue system modulo m . Hence the product of all the integer in the first set is congruent to the product of those in the second set. Therefore

$$\begin{aligned} b_1 b_2 \dots b_{\varphi(m)} &\equiv ab_1, ab_2 \dots ab_{\varphi(m)} \\ &\equiv a^{\varphi(m)} b_1 b_2 \dots b_{\varphi(m)} \pmod{m}. \end{aligned}$$

Since each b_i is relatively prime to m ($b_i, m) = 1$ for $i = 1, 2, \dots, \varphi(m)$ canceling each b_i we get $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Corollary 1 : If a prime p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$.

Taking $m = p$, $\varphi(m) = \varphi(p) = p-1$, and $(a, p) = 1$, hence the result follows from theorem 9.

PROOF OF THEOREM 8 : If a is any integer and p is any prime then two cases arise.

Either $p \mid a$ or $p \nmid a$. In the case when $p \mid a$ we get $p \mid a^p$ hence $p \mid a^p - a$, i.e. $a^p - a \equiv 0 \pmod{p}$.

Or $a^p \equiv a \pmod{p}$.

In the second case when $p \nmid a$ i.e. $(a, p) = 1$ then by the corollary we get $a^{p-1} \equiv 1 \pmod{p}$.

Multiplying by a both sides since $(a, p) = 1$, we get $a^p \equiv a \pmod{p}$.

Thus theorem 8 is proved..

SECOND PROOF OF THEOREM 8 : The proof is by induction on a . If $a = 1$ then $1^p \equiv 1 \pmod{p}$ is true as is the case $a = 0$. Assume the result hold for a , we will show it is true for $a+1$. that is to show that $(a+1)^p \equiv (a+1) \pmod{p}$ when $a^p \equiv a \pmod{p}$.

Now, by binomial theorem

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \dots + \binom{p}{1} a^p + \dots + \binom{p}{p-1} a + 1.$$

By assumption $a^p \equiv a \pmod{p}$.

We have to show that the binomial coefficients $\binom{p}{k}$ given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \text{ is divisible by } p \text{ for } k = 1, 2, \dots, p-1.$$

That is to show that

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

$$\text{Now } k! \binom{p}{k} = p!/(p-k)! = p(p-1)\dots(p-k+1) \equiv 0 \pmod{p},$$

which implies either $p \mid k!$ or $p \mid \binom{p}{k}$. But $p \mid k!$ is impossible since $1 \leq k \leq p-1$.

$$\text{Hence } p \mid \binom{p}{k} \text{ i. e. } \binom{p}{k} \equiv 0 \pmod{p}.$$

Hence we have

$$(a+1)^p \equiv a^p + 1 \equiv (a+1) \pmod{p}.$$

Hence the theorem follows when $a \geq 0$. If a is a negative integer, there is no problem since $a \equiv r \pmod{p}$ for some r , where $0 \leq r \leq p-1$.

We get $a^p \equiv r^p \equiv r \equiv a \pmod{p}$.

THEOREM 10 : If p is prime, then $(x+y+\dots+w)^p \equiv x^p + y^p + \dots + w^p \pmod{p}$.

PROOF : $(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \dots + \binom{p}{p-1} x y^{p-1} + y^p \equiv x^p + y^p \pmod{p},$

since $\binom{p}{k}$, $k = 1, 2, 3, \dots, p-1$ is divisible by p ,

the general result follows by the repetition of the argument.

Corollary 2 : $a^p \equiv a \pmod{p}$ (Little Fermat's theorem).

By taking $x = y = z = \dots = w = 1$ in theorem 11 if there are a number we get

$$(1+1+\dots+a)^p \equiv 1^p + 1^p \dots \text{ to } a \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}.$$

THEOREM 11 : If $\alpha > 0$ and $m \equiv 1 \pmod{p^\alpha}$

$$\text{then } m^p \equiv 1 \pmod{p^{\alpha+1}}$$

PROOF : $m \equiv 1 \pmod{p^\alpha} \Rightarrow$

$$m = 1 + kp^\alpha, k \text{ is an integer, and } \alpha p \geq \alpha + 1.$$

Hence

$$m^p = (1 + kp^\alpha)^p = 1 + l p^{\alpha+1} \text{ where } l \text{ is an integer.}$$

Corollary 3 : $a^{p(p-1)} \equiv 1 \pmod{p^2},$

$$a^{p^2(p-1)} \equiv 1 \pmod{p^2}, a^{p^{(\alpha-1)}(p-1)} \equiv 1 \pmod{p^2}$$

Taking $m = a^{p-1}$ in theorem 11 we have $a^{p-1} \equiv 1 \pmod{p}$ then we get $a^{p(p-1)} \equiv 1 \pmod{p^2}$. Again taking $m = a^{p(p-1)}$ and $\alpha = 2$ we get

$a^{p^2(p-1)} \equiv 1 \pmod{p^2}$ and so on. Hence proved.

Example 1 : $11 \mid 5^{38} - 4$.

By Fermat's theorem $5^{10} \equiv 1 \pmod{11}$ since $(5, 11) = 1$.

$$\begin{aligned} \text{Now } 5^{38} &= 5^{10 \times 3 + 8} = (5^{10})^3 (5^2)^4 \\ &\equiv 1 \cdot (25)^4 \equiv 1 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}. \end{aligned}$$

$$\text{Since } 25 \equiv 3 \pmod{11}$$

$$\text{Hence } 11 \mid 5^{38} - 4.$$

Example 2 : Find the unit digit of 3^{100} , by Fermat's theorem.

Fermat's theorem gives $3^4 \equiv 1 \pmod{5}$, $3^4 \equiv 1 \pmod{2}$.

$$\begin{aligned} \text{These two} \quad &\Rightarrow 3^4 \equiv 1 \pmod{10} \\ &\Rightarrow 3^{100} \equiv 1 \pmod{10} \\ &\Rightarrow 1 \text{ is the unit digit in } 3^{100}. \end{aligned}$$

Example 3 : Find the last two digits of 3^{100} .

$$\text{Since } (3, 100) = 1, \quad 3^{\phi(100)} \equiv 1 \pmod{100}$$

$$\text{But } \phi(100) = 40. \text{ We have}$$

$$\begin{aligned} 3^{40} &\equiv 1 \pmod{100} \\ 3^{100} &= 3^{40 \cdot 2 + 20} = (3^{40})^2 3^{20} \\ &\equiv 3^{20} \pmod{100} \\ &\equiv (3^5)^4 \pmod{100} \\ &\equiv (43)^4 \pmod{100} \equiv (1849)^2 \pmod{100} \\ &\equiv (49)^2 \pmod{100} \\ &\equiv 01 \pmod{100}. \end{aligned}$$

Example 4 : Determine the last two digits of 1999^{1999} .

We need congruence $1999^{1999} \pmod{100}$.

$$\phi(100) = \phi(25) \phi(4) = 40.$$

$$1999 = 40k + 39, \quad 1999 \equiv 39 \pmod{100}$$

$$1999^4 \equiv 1 \pmod{100} \text{ (By Euler's-Fermat's theorem)}$$

$$1999^{40k} \equiv 1 \pmod{100}.$$

Hence $1999^{40k+39} \equiv (99)^{39} \pmod{100}$.

(By Euler–Fermat theorem) $99^{40} \equiv 1 \pmod{100}$.

To find $(99)^{39} \pmod{100}$

$$99 \equiv -1 \pmod{100}$$

Hence $(99)^{39} \equiv (-1)^{39} \pmod{100}$

$$\equiv -1 \pmod{100} \equiv 99 \pmod{100}$$

That is, the last two digits are 99.

Example 5 : Find the last two digits of $N = 123^{456}$.

Solution : $123 \equiv 23 \pmod{100}$. We know $a^{2^{n+1}} = (a^{2^n})^2$

We have $456 = 256 + 128 + 64 + 8$.

$$123 \equiv 23 \pmod{100}$$

$$(123)^2 \equiv 23^2 = 529 \equiv 29 \pmod{100}$$

$$(123)^4 \equiv 29^2 \equiv 41 \pmod{100}$$

$$(123)^8 \equiv 41^2 \equiv 81 \pmod{100}$$

$$(123)^{16} \equiv 81^2 \equiv 61 \pmod{100}$$

$$(123)^{32} \equiv 61^2 \equiv 21 \pmod{100}$$

$$(123)^{64} \equiv 21^2 \equiv 41 \pmod{100}$$

$$(123)^{128} \equiv 41^2 \equiv 81 \pmod{100}$$

$$(123)^{256} \equiv 81^2 \equiv 61 \pmod{100}.$$

Therefore $123^{456} \equiv 123^{256+128+64+8} \equiv 61. 81.41. 81 = 16409061 \equiv 61 \pmod{100}$

Exercise : Determine the remainder when 2^{720} is divided by 225.

We can use for Euler–Fermat theorem to find the inverse of a mod m , we define the inverse of a mod m as:

Let m be a fixed integer. The arithmetic inverse of a given integer a such that $(a, m) = 1$ is an integer a^* such that $aa^* \equiv 1 \pmod{m}$.

The integer a^* is called as inverse of a mod m .

Example 2 : If $m = 10$, the inverse of 3 is 7 since $3.7 = 21 \equiv 1 \pmod{10}$.

Since $a^{\phi(m)} \equiv a.a^{\phi(m)-1} \equiv 1 \pmod{m}$, $a^{\phi(m)-1}$ is an inverse of a modulo m .

Example 3 : If $m = 35$, $\phi(35) = \phi(7) \cdot \phi(5) = 6 \cdot 4 = 24$. Hence $2^{24} \equiv 1 \pmod{35}$.

The inverse of 2 mod 35 must be $2^{23} \pmod{35}$.

To calculate $2^{23} \pmod{35}$

$$2^6 \equiv 1 \pmod{7} \Rightarrow 2^{12} \equiv 1 \pmod{7}$$

$$2^4 \equiv 1 \pmod{5} \Rightarrow 2^{12} \equiv 1 \pmod{5}$$

These two imply $2^{12} \equiv 1 \pmod{35}$.

$$2^{23} = 2^{12+11} \pmod{35} \equiv 2^{11} \pmod{35} \equiv 18 \pmod{35}$$

Hence the inverse of 2 mod 35 is 18.

Exercise : Determine the inverse of 3 modulo 40.

Example 4 : Express a^{37} as a product of power of a where the exponents are powers of 2.

We write 37 in base 2 as $37 = 32 + 4 + 1 =$

$$= 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$= 100101 \text{ in base 2.}$$

$$\text{Therefore } a^{37} = a^{32} \cdot a^4 \cdot a^1.$$

We describe an algorithm in which the base 2 expansion of k in a^k is implicit. The idea is to traverse the digits of k (in base 2) from right to left. Every time we encounter a 0, divide k by 2 and square a , but do not add the term to the result. If k is odd, we multiply the result by the current power of a and subtract 1 from k .

ALGORITHM (Exponential modulo m) Given integers, k and m this algorithm compute $a^k \pmod{m}$ for $k > 0$.

1. [Initialize] set result = 1
2. [Check if done]. If $k = 0$, return result and terminate.
3. [k is odd]. If $k \bmod 2 = 1$, then let result = (result a) mod m ; $k = k - 1$, and go to step 2.
4. [k is even]. Let $a = a^2 \pmod{m}$, $k = k/2$ and go to step 2.

Example 5 : Let $k = 37$, the values in the computation are as follows.

TABLE

Iteration	a	Result	k base 10	k base 2
0	a	1	37	100101
1	a	a	36	10000
2	a^2	a	18	10010
3	a^4	a	9	1001
4	a^4	a^5	8	1000
5	a^8	a^5	4	100
6	a^{16}	a^5	2	10
7	a^{32}	a^5	1	1
8	a^{32}	a^{37}	0	0

APPLICATION OF THE METHOD OF COMPUTING $a^k \text{ MOD } m$

We will apply this method to determine if a number n is a prime power. If $n = p^k$, Fermat's theorem implies that $a^n \equiv a \pmod{p}$, then $d = (a^n - a, n)$ is divisible by p . If d is not prime then it is a power of prime we now check if d is a power of prime, if it is, then we can repeatedly divide n by this prime to see if n is a prime number. In the computation of d , it is sufficient to compute $a^n - a \text{ mod } n$.

Suppose $n = 28561$ and $a = 2$, $a^n - a \text{ mod } n = 2^n - 2 \pmod{28561}$

$= 4810$, $(4810, n) = 13$. Hence n could be a power of 13.

Repeatedly dividing n by 13 we have $n = 13^4$.

Example 6 : Find the last two digits in the decimal representation of 3^{256} .

Solution : To find $3^{256} \pmod{100}$.

Now $\phi(100) = 40$,

$$3^{40} \equiv 1 \pmod{100} \quad 256 = 6 \times 40 + 16$$

$$3^{256} \equiv 3^{6 \times 40 + 16} \equiv (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100}$$

$$\text{Now } 3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2$$

$$\equiv (61)^2 \equiv 21 \pmod{100}.$$

Now the question is whether the converse of Fermat's theorem is true or not. That is $a^n \equiv 1 \pmod{n}$ implies n is a prime. This is not true.

For example if $n = 117, a = 2$, we write

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} 2^5$$

$$\text{and } 2^7 = 128 \equiv 11 \pmod{117},$$

$$\text{we have } 2^{117} \equiv 11^{16} 2^5 \equiv (121)^8 2^5 \equiv 4^8 2^5 \equiv 2^{21} \pmod{117}$$

$$\text{But } 2^{21} = (2^7)^3 \text{ which gives}$$

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

We finally get

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

so that 117 is composite and $117 = 13 \cdot 9$. The converse of Fermat's theorem is not true. That is $a^{n-1} \equiv 1 \pmod{n}$ for some integer a then n need not be a prime. We will illustrate it by an example. For this we require the following lemma.

LEMMA : If p and q are distinct primes such that $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

PROOF : It is known from Fermat's theorem $(a^q)^p \equiv a^q \pmod{p}$ while $a^q \equiv a \pmod{p}$ by hypothesis. Combining these two we get $a^{pq} \equiv a \pmod{p}$ or $p \mid a^{pq} - a$.

Similarly $q \mid a^{pq} - a$. This yields $pq \mid a^{pq} - a$ which we write $a^{pq} \equiv a \pmod{pq}$.

Example : We will now show that $2^{340} \equiv 1 \pmod{341}$ where $341 = 11 \cdot 31$, a composite number.

$$2^{10} = 1024 = 31 \cdot 33 + 1. \text{ Thus } 2^{11}$$

$$= 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

$$\text{and } 2^{31} = 2 (2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$$

$$\text{By the lemma, } 2^{11} 2^{31} \equiv 2 \pmod{11 \cdot 31}$$

$$\text{or } 2^{341} \equiv 2 \pmod{341}.$$

After canceling common factor 2 we get $2^{340} \equiv 1 \pmod{341}$

So that the converse of Fermat's theorem fails.

3.4. LINEAR CONGRUENCES

Polynomial congruences are analogous to the polynomial equation in algebra. We consider the polynomial with integer coefficients so that the values of these polynomial will be integers when x is an integer. Consider $f(x) \equiv 0 \pmod{m}$, x, m integers. Then x is called as a solution of the congruence. By the properties of congruence if $x \equiv y \pmod{m}$ then $f(x) \equiv f(y) \pmod{m}$. So

every congruence having one solution has infinitely many solutions, we will consider solutions which are distinct and incongruent modulo m . So the number of solutions are contained in the set $\{1, 2, \dots, m\}$ or any other complete residue system modulo m . So it is expected as in case of polynomial in algebra that every polynomial congruence modulo m has at most m solutions. But it is not always true. There are some polynomial congruences which have no solution. A polynomial congruence of degree one is called as linear congruence.

Example : The linear congruence $2x \equiv 3 \pmod{4}$ and $2x \equiv 1 \pmod{2}$ have no solution, since $2x - 3$ is odd for every x and can not be divisible by 4. Similarly in other case $2x - 1$ is odd and can not be divisible by 2.

Example : A quadratic congruence $x^2 \equiv 1 \pmod{8}$ has exactly four solutions i.e. has more solutions than the degree of the polynomial congruence i.e. 2. The solutions are given by $x \equiv 1, 3, 5, 7 \pmod{8}$.

We will consider now linear congruences, we will see when it has exactly one solution, what is the condition that it must have solution and what is total number of solutions and how to find these solutions.

THEOREM 12 : Assume $(a, m) = 1$. Then the linear congruence

(2) $ax \equiv b \pmod{m}$ has exactly one solution.

PROOF : As the distinct incongruent solutions modulo m are among the CRS mod m , we test the numbers $1, 2, \dots, m$. Now form the product with a i.e. $a, 2a, \dots, ma$. Since $(a, m) = 1$ by theorem 6 these numbers also constitute a CRS modulo m . That is there is one x satisfying (2) i.e. $ax \equiv b \pmod{m}$.

Hence proved.

This theorem tells us the existence of exactly one solution but it does not say anything about how to determine this solution. If $(a, m) = 1$ then the unique solution of the congruence $ax \equiv 1 \pmod{m}$ is the reciprocal of a mod m . About the reciprocal we have already studied in the section 3.3.

To see the necessary and sufficient condition for the congruence (2) has solutions.

THEOREM 13 : Assume $(a, m) = d$. Then the linear congruence (2) has solution if, and only if, $d \mid b$.

PROOF : If a solution of linear congruence (2) exists then $(a, m) = d$ implies $d \mid m$ and $d \mid a$. Hence $d \mid ax - my = b$ i.e. $d \mid b$.

Conversely dividing the congruence (2) $ax \equiv b \pmod{m}$ by d , we get

$$(3) \quad \begin{aligned} a/d \cdot x &\equiv b/d \pmod{m/d} \text{ and} \\ (a, m) = d &\Rightarrow (a/d, m/d) = 1. \end{aligned}$$

Therefore by theorem 12 congruence (3) has exactly one solution which is also a solution of (2).

Example : $2x \equiv 3 \pmod{4}$ has no solution because $(2,4) = 2$ and $2 \nmid 3$.

THEOREM 14 : Assume $(a, m) = d$ and suppose that $d \mid b$. Then the linear congruence (2) has exactly d solutions modulo m . These are given by

$$(4) \ t, t + m/d, t + 2m/d, \dots, t + (d-1)m/d,$$

where t is the solution unique modulo m/d , of the linear congruence (2).

PROOF : A solution of (3) is a solution of (2) since if x satisfies (3) i.e. $a/d x \equiv b/d \pmod{m/d}$ then multiplying through out by d , we get $ax \equiv b \pmod{m}$ i.e. (2) is satisfied conversely if (2) is satisfied then (3) is satisfied. That is if x satisfies.

$$ax \equiv b \pmod{m}$$

and since $(a, m) = d$, dividing by d we get $a/d x \equiv b/d \pmod{m/d}$ i.e. (3) is satisfied.

Now the d number of solution given in the set (4) are of the solution of (3) hence of (2). No two of these are congruent modulo m since the relation.

$$t + r m/d \equiv t + s m/d \pmod{m},$$

with $0 \leq r < d, 0 \leq s < d$. imply

$$r m/d \equiv s m/d \pmod{m}$$

and hence,

$$r \equiv s \pmod{d} \text{ i.e. } d \mid r-s \text{ but } |r-s| < d \text{ so } r = s.$$

Next to show that the linear congruence (2) has no solution except those listed in (4). If y is a solution of (2) then $ay \equiv at \pmod{m}$ so $y \equiv t \pmod{m/d}$ by cancellation law. That is $y = t + km/d$ for some integer k . But $k \equiv r \pmod{d}$ for some r satisfying $0 \leq r < d$. Therefore

$$k m/d \equiv r m/d \pmod{m}.$$

So $y \equiv t + rm/d \pmod{m}.$

Therefore y is congruent modulo m to one of the number in the set (4). This completes the proof.

Now we will establish a theorem for determining all solution of the linear congruence. For this we use Euler-Fermat theorem.

THEOREM 15 : If $(a, m) = 1$ the solution (unique mod m) of the linear congruence

$$(5) \quad ax \equiv b \pmod{m} \text{ is given by}$$

$$(6) \quad x \equiv ba^{\phi(m)-1} \pmod{m}.$$

PROOF : The number x given by (6) satisfies (5) because

$$ax \equiv a \cdot ba^{\phi(m)-1} \pmod{m}$$

$$\equiv ba^{\phi(m)} \pmod{m}$$

$$\equiv b \pmod{m}$$

by Euler–Fermat theorem. Since $(a, m) = 1$ the solution is unique mod m . If $(a, m) = d$ we get d number of solution $t = k m/d$, $k = 0, 1, 2, 3, \dots, (d-1)$ and t is given by (6). We illustrate these by examples.

Example 1 : Solve the congruence $3x \equiv 5 \pmod{20}$.

Solution : Since the $\text{g.c.d.}(3, 20) = 1$, there is unique solution mod 20. By (5) the solution is

$$x \equiv 5 \cdot 3^{\phi(20)-1} \equiv 5 \cdot 3^7 \pmod{20}$$

But $3^4 \equiv 1 \pmod{20}$

and $3^7 \equiv 3^3 \pmod{20}$

so $x \equiv 5 \cdot 3^3 \pmod{20}$

$$\equiv 5 \times 27 \pmod{20}$$

$$\equiv 15 \pmod{20}.$$

The solution is $15 \pmod{20}$.

Example 2 : Solve $27x \equiv 45 \pmod{180}$.

Solution : Since $d = (27, 180) = 9$, and $9 \mid 45$,

so the congruence has 9 solution modulo 180.

Dividing by 9 we get

$$3x \equiv 5 \pmod{20}, \text{ which has solution } 15.$$

The solutions are given by

$$x = 15 + 20k, k = 0, 1, 2, 3, 4, 5, 6, 7, 8$$

They are

$$x \equiv 15, 35, 55, 75, 95, 115, 135, 155, 175, \pmod{180}.$$

Example 3 : Solve the linear congruence $9x \equiv 12 \pmod{15}$.

Solution : $d = (9, 15) = 3$

The linear congruence has solution since $3 \mid 12$ and it has 3 solutions.

Dividing the congruence by 3 we get

$$3x \equiv 4 \pmod{5}.$$

The solution of this linear congruence is

$$x \equiv 4.3^{\phi(5)-1} \pmod{5} = 4.3^3 \pmod{5} \equiv 3 \pmod{5}.$$

Hence the solution of the given linear congruence are

$$3 + 5k, k = 0, 1, 2. \text{ i.e. are } 3, 8, 13 \pmod{15}.$$

3.5. POLYNOMIAL CONGRUENCES MODULO p , LAGRANGE'S THEOREM :

The fundamental theorem of algebra states that every polynomial $f(x)$ of degree $n \geq 1$ the equation $f(x) = 0$ has n solution. There is no direct analog of this theorem for polynomial congruences. We have already shown in examples that some linear congruences have no solutions, some have exactly one solution and some have more than one. However, for congruences modulo a prime p we have the following theorem which guarantees p number of solutions of the congruence $f(x) \equiv 0 \pmod{p}$.

THEOREM 16 : (Lagrange)

Let $f(x) = c_0 + c_1 x + \dots + c_n x^n$ be a polynomial of degree n with integer coefficients such that $c_n \not\equiv 0 \pmod{p}$, p is a prime. Then the polynomial congruence

$$(7) \quad f(x) \equiv 0 \pmod{p}$$

has at most n solutions.

PROOF : We use the induction on n , the degree of f . When $n = 1$ the congruence is linear $c_1 x + c_0 \equiv 0 \pmod{p}$.

Since $c_1 \not\equiv 0 \pmod{p}$ i.e. $(c_1, p) = 1$, it has exactly one solution. Assume that the theorem is true for polynomials of degree $n - 1$. Suppose that the equation (7) has $n + 1$ incongruent solution modulo p , say $x_0, x_1 \dots x_n$. i.e. $f(x_k) \equiv 0 \pmod{p}$ for each $k = 0, 1, \dots, n$.

$$\begin{aligned} \text{Now} \quad f(x) - f(x_0) &= c_0 + c_1 x + \dots + c_n x^n \\ &\quad - (c_0 + c_1 x_0 + \dots + c_n x_0^n) \\ &= c_1 (x - x_0) + \dots + c_n (x^n - x_0^n) \\ &= (x - x_0) g(x), \end{aligned}$$

where $g(x)$ is a polynomial of degree $n-1$ with integer coefficients. By our assumption $g(x)$ has $(n-1)$ solutions. Thus

$$f(x_k) - f(x_0) = (x_k - x_0) f(x_k) \equiv 0 \pmod{p}$$

since

$$f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}.$$

But $x_k - x_0 \equiv 0 \pmod{p}$ if $k \neq 0$.

So we must have $g(x_k) \equiv 0 \pmod{p}$ for each $k \neq 0$.

That is $g(x) \equiv 0 \pmod{p}$ has n incongruent solutions modulo p contradicting our induction hypothesis. This completes the proof.

Remark : The theorem fails if we replace prime modulo p by a composite modulo m . For example $x^2 \equiv 1 \pmod{8}$ has four solutions 1, 3, 5, 7, instead of two solutions.

3.6. APPLICATION OF LAGRANGE'S THEOREM :

We will describe here some applications of Lagrange's Theorem.

THEOREM 17 : If $f(x) = c_0 + c_1 x + \dots + c_n x^n$ is a polynomial of degree n with integer coefficients and if the congruence $f(x) \equiv 0 \pmod{p}$ has more than n solutions, where p is prime, then every coefficient of f is divisible by p .

PROOF : Suppose the theorem is not true. Let c_k be the one coefficient with largest index which is not divisible by p i.e. $p \nmid c_k$, $k \leq n$. Then the congruence

$$c_0 + c_1 x + \dots + c_k x^k \equiv 0 \pmod{p}$$

has more than k solutions. So, by Lagrange's theorem $p \nmid c_k$ which is a contradiction. Hence all the coefficients of $f(x)$ are divisible by p . Hence proved,

THEOREM 18 : For any prime p all the coefficients of the polynomial

$$f(x) = (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1$$

PROOF : Let $g(x) = (x-1)(x-2)\dots(x-p+1)$ and $h(x) = x^{p-1} - 1$. Then $f(x) = g(x) - h(x)$.

The roots of $g(x)$ are $1, 2, \dots, p-1$.

Hence $g(x)$ satisfies the congruence $g(x) \equiv 0 \pmod{p}$.

Now by Euler-Fermat theorem

$$x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^{p-1} - 1 \equiv 0 \pmod{p}.$$

That is $h(x) \equiv 0 \pmod{p}$. It has $p-1$ roots.

Now $f(x) = g(x) - h(x) \equiv 0 \pmod{p}$.

By Lagrange's theorem it must have the $p-1$ number of solutions.

But

$$\begin{aligned} f(x) &= (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1 \\ &= x^{p-1} + c_1 x^{p-2} + \dots + (p-1)! - x^{p-1} + 1 \\ &= f_1(x), \end{aligned}$$

where $f_1(x)$ is a polynomial of degree $p-2$ so $f(x)$ is a polynomial of degree $p-2$ having $p-1$ roots implies by theorem 18 that all its coefficients are divisible by p .

THEOREM 19 : (Wilson's theorem) For any prime p we have

$$(p-1)! + 1 \equiv 0 \pmod{p} \text{ or } (p-1)! \equiv -1 \pmod{p}.$$

PROOF : Let $f(x) = (x-1)(x-2) \dots (x-p+1) - x^{p-1} + 1$

On expanding $f(x)$ we get

$$f(x) = x^{p-1} + c_1 x^{p-2} + \dots + c_{p-2} x + c_{p-1} - x^{p-1} + 1$$

where $c_{p-1} + 1$ is the constant term of $f(x)$ that is $c_{p-1} + 1 = (p-1)! + 1$.

Since by theorem 18 all the coefficients of $f(x)$ are divisible by p , hence

$$c_{p-1} + 1 = (p-1)! + 1 \equiv 0 \pmod{p}$$

$$\text{i.e. } (p-1)! \equiv -1 \pmod{p}$$

which proves Wilson's theorem.

SECOND PROOF OF WILSON'S THEOREM : We can prove this theorem without using Lagrange's theorem.

If $p = 2$ and $p = 3$ the theorem is trivial. Since $1! + 1 \equiv 0 \pmod{2}$ and $2! + 1 \equiv 0 \pmod{3}$ let us take $p > 3$. Suppose that a is any one of the $p-1$ positive integers,

$$1, 2, 3, \dots, p-1$$

and consider the linear congruence $ax \equiv 1 \pmod{p}$.

Then $\gcd(a, p) = 1$. Hence the linear congruence has unique solution modulo p ; hence there is a unique integer a^* , with $1 \leq a^* \leq p-1$, satisfying

$$a a^* \equiv 1 \pmod{p}.$$

Since p is prime $a = a^*$ if and only if $a = 1$ or $a = p-1$. The congruence

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow (a-1)(a+1) \equiv 0 \pmod{p}.$$

Therefore either $a-1 \equiv 0 \pmod{p}$ in which case $a = 1$ or $a+1 \equiv 0 \pmod{p}$ in which case $a = p-1$. If we will consider $a = 1$ and $a = p-1$ and group the remaining integers $2, 3, \dots, p-2$ into pairs a, a' where $a \neq a'$ such that $a a' \equiv 1 \pmod{p}$. There are $(p-3)/2$ congruences are multiplied together and rearranged we get

$$2.3 \dots (p-2) \equiv 1 \pmod{p}$$

$$\Rightarrow (p-2)! \equiv 1 \pmod{p}.$$

Multiplying by $p-1$ we get

$$(p-1)(p-2)! = (p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

i.e. $(p-1)! \equiv -1 \pmod{p}$

which proves Wilson's theorem.

CONVERSE OF WILSON'S THEOREM :

The converse of Wilson's theorem states that: If $(n-1)! \equiv -1 \pmod{n}$, then n is a prime.

PROOF : If n is not prime, then n has a divisor d with $1 < d < n$. Since $d \leq n-1$, d occurs as one of the factors in $(n-1)!$ whence $d \mid (n-1)!$. By hypothesis $n \mid (n-1)! + 1$ since $d \mid n$, these two together imply that $d \mid (n-1)! + 1$.

But $d \mid (n-1)!$ hence $d \mid 1$ which is not true.

Remark : Wilson's theorem and its converse theorem provide us with necessary and sufficient conditions for determining primality of an integer. We say that $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. We now apply Wilson's theorem to study the quadratic congruences. $ax^2 + bx + c \equiv 0 \pmod{n}$ with $(a, n) = 1$.

THEOREM 20 : The quadratic congruences $x^2 + 1 \equiv 0 \pmod{p}$ where p is a prime, has solutions if and only if $p \equiv 1 \pmod{4}$ i.e. $p = 4k + 1$, $k = 1, 2, 3, \dots$

PROOF : Let a be any solution of $x^2 + 1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$.

Since $p \nmid a$, Fermat's theorem gives

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

If $p = 4k + 3$ then R.H.S is -1 and

$$1 \equiv -1 \pmod{p} \Rightarrow p \mid 2$$

which is impossible. Hence p can not be $4k + 3$.

Therefore p is of the form $4k + 1$.

Converse part

Now

$$(p-1)! = 1.2.....(p-1/2)(p+1/2) \dots (p-2)(p-1)$$

we have

$$(p-1) \equiv -1 \pmod{p}$$

$$(p-2) \equiv -2 \pmod{p}$$

$$(p+1)/2 \equiv (p-1)/2 \pmod{p}$$

Rearranging the factors, we get

$$(p-1)! \equiv 1 (-1) (-2) \dots ((p-1)/2) (-(p-1)/2) \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} (1.2 \dots (p-1)/2) \pmod{p}$$

since there are $(p-1)/2$ minus sign is involved.

By Wilson's theorem

$$(p-1)! \equiv -1 \pmod{p}.$$

Putting this value we get

$$-1 \equiv (-1)^{\frac{p-1}{2}} [(p-1)/2!]^2 \pmod{p}.$$

If $p = 4k + 1$ then $(-1)^{\frac{p-1}{2}} = 1.$

Hence $-1 \equiv [(p-1)/2!]^2 \pmod{p}$

i.e. $[(p-1)/2]!$ satisfying the quadratic congruence

$$x^2 + 1 \equiv 0 \pmod{p}.$$

Example 1 : $p = 17$ p is of the form $4k + 1$. $(p-1)/2 = 8$ and $8! \equiv 40320 \equiv 13 \pmod{17}$,

Hence $13^2 + 1 \equiv 0 \pmod{17}$.

Example 2 : If p is odd, $p > 1$, prove that $1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{p+1/2} \pmod{p}$

and $2^2 \cdot 4^2 \cdot 6^2 \dots (p-1)^2 \equiv (-1)^{p+1/2} \pmod{p}$

Example 1 gives that if p is an odd prime and if $q = p-1/2$ then

$$((p-1/2)!)^2 + (-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p} \text{ if } p = 4k + 1.$$

Since $k \equiv -(p-k) \pmod{p}$ it follows that

$$2 \cdot 4 \cdot 6 \dots (p-1) \equiv (-1)^{\frac{p-1}{2}} 1 \cdot 3 \cdot 5 \dots (p-2) \pmod{p}.$$

Squaring we get,

$$2^2 \cdot 4^2 \cdot 6^2 \dots (p-1)^2 \equiv (-1)^{p-1} 1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \pmod{p}.$$

Since p is odd $p+1/2$ is even and $p-1$ is even,

hence $2^2 \cdot 4^2 \cdot 6^2 \dots (p-1)^2 \equiv 1^2 \cdot 3^2 \cdot 5^2 \dots (p-2)^2 \equiv (-1)^{p+1/2} \pmod{p}$.

Excercise : For a prime p of the form $4k + 3$, prove that either

$(p-1/2)! \equiv 1 \pmod{p}$ or $(p-1/2)! \equiv -1 \pmod{p}$ hence $(p-1/2)!$ satisfies the quadratic congruence $x^2 \equiv 1 \pmod{p}$.

Solution : By Wilson's Theorem $-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} [(p-1/2)!]^2 \pmod{p}$.

$$\equiv (-1)^{2k+1} [(p-1/2)!]^2 \pmod{p}$$

(since $p = 4k + 3$)

$$\equiv - [(p-1/2)!]^2 \pmod{p}.$$

$$\Rightarrow [(p-1/2)!]^2 \equiv 1 \pmod{p}$$

$$\Rightarrow ((p-1/2)! + 1)((p-1/2)! - 1) \equiv 0 \pmod{p}$$

$$\Rightarrow (p-1/2)! \equiv -1 \pmod{p} \text{ or } (p-1/2)! \equiv 1 \pmod{p}.$$

Exercise : Find all positive integers n for which $(n-1)! + 1$ is a power of n .

Solution : If $n = p$ then the congruence $(p-1)! + 1 \equiv 0 \pmod{p^2}$ is true for $p = 5, p = 13, p = 563$. But no other value of $p < 200000$.

If n is a composite then $(n-1)! + 1 \equiv 0 \pmod{n^2}$ is not true.

For example take

$$n = 6$$

$$36 \nmid 5! + 1.$$

3.7. SIMULTANEOUS LINEAR CONGRUENCES, THE CHINESE REMAINDER THEOREM AND ITS APPLICATIONS

THEOREM 21 : Let m_1, m_2, \dots, m_r be pairwise relatively prime integers and $M = m_1 m_2 \dots m_r$. Then for integers b_1, b_2, \dots, b_r the system of congruences

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$x \equiv b_k \pmod{m_k}$$

$$x \equiv b_r \pmod{m_r}$$

has a simultaneous solution which is unique modulo M .

PROOF : $M = m_1 m_2 \dots m_r$.

Let $M_k = M/m_k = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$. Then $(M_k, m_k) = 1$ so that M_k has a unique reciprocal M_k' modulo m_k .

That is $M_k M_k' \equiv 1 \pmod{m_k}$.

Now let $x = b_1 M_1 M_1' + b_2 M_2 M_2' + \dots + b_r M_r M_r'$.

Consider each term in this sum modulo m_k . Since

$$M_i \equiv 0 \pmod{m_k} \text{ if } i \neq k$$

we have

$$x \equiv b_k M_k M_k' \equiv b_k \pmod{m_k}.$$

Hence x satisfies every congruence in the system. But it is easy to show that the system has only one solution mod m . In fact, if x and y are two solutions of the system we have $x \equiv y \pmod{m_k}$ for each k and since the m 's are relatively in pairs, we also have $x \equiv y \pmod{M}$. This completes the proof.

THEOREM 22 : Let m_1, m_2, \dots, m_r be relatively prime in pairs. Let b_1, b_2, \dots, b_r be arbitrary integers and let a_1, a_2, \dots, a_r satisfy $(a_k, m_k) = 1$, for $k = 1, 2, \dots, r$. Then the linear system of congruences

$$(8) \quad \begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

has exactly one solution modulo $M = m_1 m_2 \dots m_r$.

PROOF : Since $(a_k, m_k) = 1$ for $k = 1, 2, \dots, r$,

then there exist a_k' such that $a_k a_k' \equiv 1 \pmod{m_k}$ and a_k' is the reciprocal of a_k .

Then the linear congruence

$$a_k x \equiv b_k \pmod{m_k} \Leftrightarrow x \equiv b_k a_k' \pmod{m_k}.$$

Now we apply theorem 15 to the system of congruences

$$x \equiv b_k a_k' \pmod{m_k}, k = 1, 2, \dots, r.$$

which has a unique solution modulo M i.e. $x \equiv b_k a_k' M_k M_k' \equiv b_k a_k' \pmod{m_k}$

which satisfy the given system of linear congruences.

Example 1 : Find all x which simultaneously satisfy system of congruences.

$$x \equiv 1 \pmod{3},$$

$$x \equiv 2 \pmod{4}$$

$$x \equiv 3 \pmod{5}$$

Solution :

$$m_1 = 3, m_2 = 4, m_3 = 5$$

$$M = m_1 m_2 m_3 = 60 \quad M_1 = 60/3 = 20$$

$$M_2 = 60/4 = 15, M_3 = 60/5 = 12.$$

To find the reciprocals of $M_1 \pmod{m_1}$, $M_2 \pmod{m_2}$ and $M_3 \pmod{m_3}$.

$$\text{Since } 20 \times 2 \equiv 1 \pmod{3} \Rightarrow M_1^{-1} = 2$$

$$15 \times 3 \equiv 1 \pmod{4} \Rightarrow M_2^{-1} = 3$$

$$12 \times 3 \equiv 1 \pmod{5} \Rightarrow M_3^{-1} = 3.$$

Hence
$$x \equiv 1 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3 \equiv 238 \pmod{60}$$
$$\equiv 58 \pmod{60}.$$

So the unique solution is $58 \pmod{60}$. We can verify that 58 satisfies the three linear congruences.

Example 2 : Determine the smallest positive integer that gives a remainder of 2 upon division by 3, a remainder of 1 upon division by 5, and a remainder of 6 upon division by 7.

Solution : Let x be a solution. Then the condition requires that

$$x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 6 \pmod{7}$$

$$M = 3 \times 5 \times 7 = 105.$$

$$M_1 = 35, M_2 = 21 \text{ and } M_3 = 15.$$

Now we will determine the inverses of $M_i, i = 1, 2, 3$,

Now

$$35 \times 2 \equiv 1 \pmod{3} \Rightarrow M_1' = 2$$

$$21 \times 1 \equiv 1 \pmod{5} \Rightarrow M_2' = 1.$$

$$15 \times 1 \equiv 1 \pmod{7} \Rightarrow M_3' = 1.$$

Therefore

$$x \equiv 2.35.2 + 1.21.1 + 6.15.1 \pmod{105}$$

$$\equiv 140 + 21 + 90 \pmod{105}$$

$$\equiv 251 \pmod{105}$$

$$\equiv 41 \pmod{105}.$$

One can easily verify that 41 is the smallest integer which satisfy the above linear congruences.

APPLICATION OF CHINESE REMAINDER THEOREM :

By applying Chinese remainder theorem we will solve polynomial congruences with composite moduli.

THEOREM 23 : Let f be a polynomial with integer coefficients, let m_1, m_2, \dots, m_r be positive integer relatively prime in pairs and let $m = m_1 m_2 \dots m_r$. Then the congruence

$$(9) \quad f(x) \equiv 0 \pmod{m}$$

has a solution if, and only if, each of the congruence.

$$(10) \quad f(x) \equiv 0 \pmod{m_i}, i = 1, 2, \dots, r.$$

has a solution. Moreover, if $v(m)$ and $v(m_i)$ denote the number of solution of (9) and (10) respectively, then

$$(11) v(m) = v(m_1) v(m_2) \dots v(m_r).$$

PROOF : If $f(a) \equiv 0 \pmod{m}$ then $f(a) \equiv 0 \pmod{m_i}$ for each $i = 1, 2, \dots, r$. Hence every solution of (9) is a solution of (10).

Conversely, let a_i be a solution (10). Then by the Chinese remainder theorem there exists an integer a such that

$$(12) \quad a \equiv a_i \pmod{m_i} \text{ for } i = 1, 2, \dots, r$$

$$\text{So} \quad f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}.$$

Since m_i 's are relatively prime in pairs we have $f(a) \equiv 0 \pmod{m}$. Therefore the number of integer a which is a solution of (10) is also a solution of (9). Since each a_i runs through the $v(m_i)$ solution of (10) the number of integers a which satisfy (12) and hence (10) is $v(m_1) \dots v(m_r)$. This proves (11).

THEOREM 24 : An even perfect number n ends in the digit 6 or 8 ie

$$n \equiv 6 \pmod{10}$$

$$\text{or} \quad n \equiv 8 \pmod{10}.$$

PROOF : A perfect number n is of the form $n = 2^{k-1} (2^k - 1)$, where $2^k - 1$ is a prime k must be prime. If $k = 2$, then $n = 6$. We may confine our attention to the case $k > 2$. $k = 4m + 1$ or $4m + 3$ If $k = 4m + 1$ then

$$n = 2^{4m} (2^{4m+1} - 1)$$

$$= 2^{8m+1} - 2^{4m}$$

$$= 2 \cdot 16^{2m} - 16^m$$

$$\text{But} \quad 16 \equiv 6 \pmod{10}.$$

$$\text{Hence} \quad n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}.$$

$$\text{If} \quad k = 4m + 3$$

$$n = 2^{4m+2} (2^{4m+3} - 1)$$

$$= 2^{8m+5} - 2^{4m+2}$$

$$= 2 \cdot 16^{2m+1} - 4 \cdot 16^m$$

$$\text{Since} \quad 16 \equiv 6 \pmod{10}$$

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \pmod{10}$$

$$\equiv 2 \cdot 12 \pmod{10}$$

$$\equiv 8 \pmod{10}.$$

Hence proved.

Exercise : If p is any prime other than 2 or 5, p divides infinitely many

$$(i) \ 1, 11, 111, 1111, \dots, 1111111111$$

$$(ii) \ 9, 99, 999, 9999, \dots, 99999999.$$

Solution :

$$(i) \quad 1 = 4 - 3 = 4k - 3$$

$$11 = 4 \times 2 + 3 = 4k + 3$$

$$111 = 4 \times 27 + 3 = 4k + 3$$

$$111\dots 11111 = 111 \dots 108 + 3 = 4k + 3.$$

So these numbers are divisible by primes of the form $4k + 3$ and 2 or 5 are not of the form $4k + 3$.

$$(ii) \quad 9 = 4 \times 2 + 1$$

$$99 = 4 \times 25 - 1$$

$$999 = 4 \times 250 - 1.$$

9, 99, are either of the form $4k + 1$ or $4k - 1$. So they are divisible by primes of the form $4k + 1$ or $4k - 1$ not by 2 or 5.

3.8. SOME ALGORITHMS

ALGORITHM (Chinese Remainder Theorem)

Given pair wise coprime integers m_i ($1 \leq i \leq k$) and integer x_i , this algorithm finds an integer x such that $x \equiv x_i \pmod{m_i}$ for all i .

1. [Initialize] set $i \leftarrow 1$, $m \leftarrow m_1$, $x \leftarrow x_1$.

2.[finished?] If $i = k$ output x and terminate the algorithm. Otherwise set $i \leftarrow i + 1$, and by a suitable version of Euclid's extended algorithm compute u and v such that $u m + v m_i = 1$.

3. [Compute next x] set $x \leftarrow u m x_i + v m_i x$, $m \leftarrow m m_i$, $x \leftarrow x \bmod m$ and go to step 2.

Here we give the following computer program in BASIC to solve the following congruences:

$$x \equiv 0 \pmod{5}$$

$$x \equiv 1 \pmod{7}$$

$$x \equiv 8 \pmod{9}.$$

```
100 REM CHINESE REMAINDER THEOREM
```

```
101 PRINT "I WANT YOU TO THINK A NUMBER"
```

```
102 PRINT " LESS THAN 316 WRITE THIS NUMBER"
103 PRINT " DOWN AND DIVIDE BY 5 NOW GIVE ME "
104 PRINT " THE REMAINDER LEFT OVER"
110 INPUT R5
111 PRINT
120 PRINT "NOW DIVIDE YOUR ORIGINAL NUMBER BY"
121 PRINT " 7 AND GIVE ME THIS REMAINDER"
130 INPUT R7
131 PRINT
140 PRINT " NOW DIVIDE YOUR ORIGINAL NUMBER BY"
141 PRINT "9 AND GIVE ME THIS REMAINDER"
150 INPUT R9
151 PRINT
160 REM CALCULATE NUMBER
170 LET A = 126 * R5 + 225 * R7
180 LET X = A - INT (A/315) * 315
190 PRINT
200 PRINT " I AM HAPPY TO TELL YOU THAT YOUR"
201 PRINT "NUMBER CHOSEN WAS", x
210 END
```

RUN

I WANT YOU THINK OF A NUMBER
LESS THAN 316 WRITE THIS
NUMBER DOWN AND DIVIDE BY 5.
NOW GIVE ME THE REMAINDER LEFT OVER ? 0
NOW DIVIDE YOUR ORIGINAL NUMBER BY 7
AND GIVE ME THIS REMAINDER ? 1
NOW DIVIDE YOUR ORIGINAL NUMBER BY 9
AND GIVE ME THIS REMAINDER ? 8
I AM HAPPY TO TELL YOU
THAT YOUR NUMBER CHOSE N WAS 260.

EXERCISE

1. Find the remainders when 2^{50} and 41^{65} are divided by 7.
2. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39 and that $111^{333} + 333^{111}$ is not divisible by 7.
3. If p is a prime satisfying $n < p < 2n$, show that $\binom{2n}{n} \equiv 0 \pmod{p}$.
4. For $n \geq 1$, using congruence theory establish each of the following:
 - (a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$
 - (b) $13 \mid 3^{n+2} + 4^{2n+1}$
 - (c) $27 \mid 2^{5n+1} + 5^{n+2}$
 - (d) $43 \mid 6^{n+2} + 7^{2n+1}$
5. Find the remainder when 4444^{4444} is divided by 9,
6. Determine the last three digits of the number 7^{999} (Hints: $7^{4n} \equiv (1 + 400)^n \equiv 1 + 400 \pmod{100}$)
7. Find the remainder when 3^{100} is divided by 5.
8. Solve the linear congruence
 - (a) $36x \equiv 8 \pmod{102}$
 - (b) $34x \equiv 60 \pmod{98}$
 - (c) $140x \equiv 133 \pmod{301}$
 - (d) $6x \equiv 15 \pmod{21}$
9. Solve each of the following set of simultaneous equation
 - (a) $x \equiv 5 \pmod{11}$ $x \equiv 15 \pmod{31}$, $x \equiv 14 \pmod{129}$
 - (b) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$
 - (c) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$
10. Prove that $1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}$.
11. Find the remainder when $2(26!)$ is divided by 29.
12. Prove that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$.
13. Verify that $4(29!) + 5!$ is divisible by 31.
14. Show that if $p = 4k + 1$ is prime then $2[(2k)!]^2 \equiv -1 \pmod{p}$.
15. Write a computer program to solve a set of simultaneous congruences when the moduli are relatively prime.

- 16 Solve $x^2 \equiv 2 \pmod{7^2}$.
- 17 Show that $2^{50} + 3^{50}$ is divisible by 13.
- 18 Show that $7 \mid n^2 + 1$ for any n .
- 19 Determine the remainder when 2^{372} is divided by 37.
- 20 Show that $11^{81} - 5^{81}$ is divisible by 7.
- 21 Prove that each member of the set of $n-1$ consecutive integer $n! + 2, n! + 3, \dots, n! + n$ is divisible by a prime which does not divide any other member of the set.
22. Let a, b, n be positive integer such that n divide $a^n - b^n$. Prove that n also divides $(a^n - b^n) / (a - b)$.
23. Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integer n .
24. A number whose only digits are 1 is called a Repunit.
Factorize 111111111 (9-one) into product of primes.
25. Find all integral solutions of $x^2 + 1 \equiv 0 \pmod{5^2}$.
26. Find the remainder when $2^{1000000}$ is divided by 77.
27. Prove that $1 + a + a^2 + \dots + a^{\varphi(m)-1} \equiv 0 \pmod{m}$
if $\text{g.c.d}(a, m) = 1$ and $\text{g.c.d}(a-1, m) = 1$.
28. Let $\Phi n = 2^{2^n} + 1$.
(a) Prove that $\Phi n \mid (2^{2^{n+1}} - 1)$.
(b) Prove that if $a \mid b$, then $(2^a - 1) \mid (2^b - 1)$.
(c) Prove that $(2^{2^{n+1}} - 1) \mid (2^{2^{2n}} - 1)$.
29. Prove that if p denotes an odd prime, then $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$.
30. Given any positive integer k , prove that there are k consecutive integers each divisible by a square > 1 .



SOME THEOREMS ON DISTRIBUTION OF PRIME NUMBERS

4.1. INTRODUCTION :

If $x > 0$, we define $\pi(x)$ as the number of primes not exceeding x . Then $\pi(x) \rightarrow \infty$ as $x \rightarrow \infty$ since there are infinitely many primes. The behaviour of $\pi(x)$ as a function of x has been the object of intense study by many celebrated mathematicians ever since the eighteenth century. Gauss (1792) and Legendre (1798) conjectured that $\pi(x)$ is asymptotic to $x / \log x$, that is $\pi(x) \sim x / \log x$, which means

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

This conjecture is known as PRIME NUMBER THEOREM (PNT).

The proof of this PNT is given by Hadamard, and de la Vallee Pousin and are analytic in nature. In this chapter we will concern with elementary theorems on primes. We will show that PNT can be expressed in several equivalent forms. We will define in the section 4.2 some auxillary functions which help in establishing equivalent theorems of Prime Number Theorem.

4.2. CHEBYSHEV'S FUNCTION $\psi(x)$ and $\vartheta(x)$.

DEFINITION 1 : For $x > 0$ we define Chebyshev's ψ function by the formula

$$\psi(x) = \sum_{n \leq x} \Lambda(n),$$

where $\Lambda(n)$ is the Mangoldt function.

Since $\Lambda(n) = 0$, unless n is a prime power we can write the definition of $\psi(x)$ as

$$(1) \quad \psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{p^m \leq x} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} 1$$

follows:

The sum on the right of (1) is a finite sum .

For if $x^{1/m} < 2$ i.e. if $1/m \log x < \log 2$

or if $m > \log x / \log 2$

i.e. $m = [\log x / \log 2] + 1$ the sum on p is zero .

$$(2) \quad \psi(x) = \sum_{m \leq \log x / \log 2} \sum_{p \leq x^{1/m}} \log p.$$

DEFINITION 2 : if $x > 0$ we define Chebyshev's ϑ - function by the equation

$$(3) \quad \vartheta(x) = \sum_{p \leq x} \log p$$

where p runs over all prime $\leq x$.

By using (3) in (2) we get

$$\begin{aligned} \psi(x) &= \sum_{m \leq \log x / \log 2} \sum_{p \leq x^{1/m}} \log p \\ &= \sum_{m \leq \log x / \log 2} \vartheta(x^{1/m}) \\ &= \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \dots \end{aligned}$$

$$(4) \quad \Rightarrow \psi(x) - \vartheta(x) \geq 0.$$

The next theorem gives the relation between $\psi(x) / x$ and $\vartheta(x) / x$.

THEOREM 1 : For $x > 0$ we have

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x} \log 2}.$$

Further,

$$\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} = 0.$$

PROOF : From (4) we find

$$0 \leq \psi(x) - \vartheta(x) \leq \sum_{2 \leq m \leq \log x / \log 2} \vartheta(x^{1/m}).$$

But

$$\vartheta(x) = \sum_{p \leq x} \log p \leq \sum_{p \leq x} \log x \leq x \log(x).$$

Hence

$$\vartheta(x^{1/m}) \leq x^{1/m} \log x^{1/m}.$$

So

$$0 \leq \psi(x) - \vartheta(x) \leq \sum_{2 \leq m \leq \log x / \log 2} \vartheta(x^{1/m}) \log(x^{1/m})$$

$$\leq \frac{\log x}{\log 2} \sqrt{x} \log \sqrt{x}$$

$$= \frac{\log x}{\log 2} \frac{\sqrt{x}}{2} \log x$$

$$= \frac{\sqrt{x} (\log x)^2}{2 \log 2}.$$

Since $x > 0$ dividing by x we get

$$0 \leq \frac{\Psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{\sqrt{x} (\log x)^2}{x 2 \log 2} = \frac{(\log x)^2}{\sqrt{x} 2 \log 2}.$$

Taking limit $x \rightarrow \infty$, R.H.S $\rightarrow 0$.

$$\text{Hence } \lim_{x \rightarrow \infty} \left(\frac{\Psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0.$$

This implies

$$\lim_{x \rightarrow \infty} \psi(x) / x = \lim_{x \rightarrow \infty} \vartheta(x) / x.$$

The next theorem plays a key role in establishing relation between $\pi(x)$ and $\psi(x)$ and $\vartheta(x)$ and also establishing equivalent theorems of PNT.

THEOREM 2 : (Abel's identity) For any arithmetical function $a(n)$ let

$$A(x) = \sum_{n \leq x} a(n)$$

where $A(x) = 0$ if $x < 1$.

Assume that f has a continuous derivative on the interval $[y, x]$, where $0 < y < x$, then we have

$$(5) \quad \sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt.$$

PROOF : Let $k = [x]$ and $m = [y]$, $[x]$ stand for greatest integer function ie the greatest integer contained in x . We write $x = [x] + \{x\}$ where $\{x\}$ is the fractional part of x .

So $A(x) = A(k)$ and $A(y) = A(m)$.

$$\begin{aligned} \text{then } \sum_{y < n \leq x} a(n) f(n) &= \sum_{n=[y]+1}^{[x]} a(n) f(n) \\ &= \sum_{n=m+1}^k \{A(n) - A(n-1)\} f(n) \\ &= \sum_{n=m+1}^k A(n) f(n) - \sum_{n=m+1}^k A(n-1) f(n), \end{aligned}$$

Changing the variable in the second term we get

$$\begin{aligned} \sum_{y < n \leq x} a(n) f(n) &= \sum_{n=m+1}^k A(n) f(n) - \sum_{n=m}^{k-1} A(n) f(n+1) \\ &= \sum_{n=m+1}^{k-1} A(n) \{f(n) - f(n+1)\} + A(k) f(k) - A(m) f(m+1) \end{aligned}$$

$$= - \sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t) dt + A(k) f(k) - A(m) f(m+1)$$

$$= - \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t) f'(t) dt + A(k) f(k) - A(m) f(m+1)$$

(since in $[n, n+1]$, $A(t) = A(n)$)

$$= - \int_{m+1}^k A(t) f'(t) dt + A(x) f(x) - \int_k^x A(t) f'(t) dt$$

$$= A(y) f(y) - \int_y^{m+1} A(t) f'(t) dt.$$

$$= A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt$$

Hence proved.

4.3. SOME EQUIVALENT FORMS OF THE PRIME NUMBER THEOREM.

THEOREM 3 : The following relations are equivalent:

$$(6) \lim_{x \rightarrow \infty} \pi(x) \log x / x = 1$$

$$\Leftrightarrow (7) \lim_{x \rightarrow \infty} \vartheta(x) / x = 1$$

$$\Leftrightarrow (8) \lim_{x \rightarrow \infty} \psi(x) / x = 1.$$

PROOF : (7) \Leftrightarrow (8) follows from theorem 1.

To prove (6) \Leftrightarrow (7) we require the following lemmas which relate $\pi(x)$ with $\vartheta(x)$.

LEMMA 1 : For $x \geq 2$, we have

$$(9) \vartheta(x) = \pi(x) \log(x) - \int_2^x \pi(t)/t dt$$

and

$$(10) \pi(x) = \vartheta(x) / \log(x) - \int_2^x (\vartheta(t)/t \log^2 t) dt.$$

PROOF : We prove (9) and (10) by using (5).

Let $a(n)$ denote the characteristic function of the primes; then

$$a(n) = \begin{cases} 1 & \text{if } n \text{ is a prime} \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\pi(x) = \sum_{p \leq x} p = \sum_{1 < n \leq x} a(n)$$

$$\vartheta(x) = \sum_{p \leq x} \log p = \sum_{1 < n \leq x} a(n) \log n$$

Taking $f(x) = \log x$ in (5) by taking $y=1$ we obtain

$$\vartheta(x) = \sum_{1 < n \leq x} a(n) \log n$$

$$= \pi(x) \log(x) - \pi(1) \log(1) - \int_1^x \pi(t)/t \, dt,$$

which prove (9) since $\pi(t) = 0$ for $t < 2$.

Next, let $b(n) = a(n) \log n$ and write

$$\pi(x) = \sum_{3/2 < n \leq x} b(n) 1 / \log n$$

$$\vartheta(x) = \sum_{n \leq x} b(n).$$

Taking $f(x) = 1/\log x$ in (5) with $y = 3/2$, we obtain

$$\pi(x) = \vartheta(x) / \log(x) - \vartheta(3/2) / \log(3/2) - \int_1^x (\vartheta(t)/t \log^2 t) \, dt$$

which proves (10) since $\vartheta(t) = 0$ if $t < 2$.

PROOF OF THE THEOREM. We have to prove $(6) \Leftrightarrow (7)$.

First to show that $(6) \Rightarrow (7)$ we have from (9),

$$\vartheta(x) / x = \pi(x) \cdot \log(x) / x - \int_2^x \pi(t)/t \, dt.$$

Taking limit as $x \rightarrow \infty$ we obtain

$$(6) \Rightarrow \lim_{x \rightarrow \infty} \pi(x) \log x / x = 1$$

(7) follows provided we show that

$$\lim_{x \rightarrow \infty} \frac{1}{x} \int_2^x \pi(t)/t \, dt = 0.$$

Now

$$(6) \Rightarrow \pi(t)/t \, dt = O(1/\log t)$$

for $t \geq 2$ so

$$\frac{1}{x} \int_2^x \pi(t)/t \, dt = O(1) \frac{1}{x} \int_2^x \left(\frac{dt}{\log t} \right).$$

Now

$$\begin{aligned} \int_2^x dt / \log t &= \int_2^{\sqrt{x}} dt / \log t + \int_{\sqrt{x}}^x dt / \log t \\ &\leq \frac{\sqrt{x}}{\log 2} + \frac{x - \sqrt{x}}{\log \sqrt{x}}. \end{aligned}$$

So

$$\frac{1}{x} \int_2^x dt / \log t \rightarrow 0.$$

This proves $(6) \Rightarrow (7)$.

To show $(7) \Rightarrow (6)$, we know from (10)

$$\pi(x) \log x / x = \vartheta(x) / x + \log(x) / x \int_2^x (\vartheta(t)/t \log^2 t) \, dt.$$

Taking limit as $x \rightarrow \infty$ we obtain,

$$\lim_{x \rightarrow \infty} (\pi(x) \log x / x) = \lim_{x \rightarrow \infty} (\vartheta(x) / x),$$

$$+ \lim_{x \rightarrow \infty} \left(\frac{\log x}{x} \right) \int_2^x (\vartheta(t)/t \log^2 t) dt.$$

In order to show (7) \Rightarrow (6) it is sufficient to show that

$$\lim_{x \rightarrow \infty} (\log(x)/x) \int_2^x (\vartheta(t)/t \log^2 t) dt = 0.$$

But (7) $\Rightarrow \vartheta(t) = 0(t)$ so

$$\frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt = 0 \left(\frac{\log x}{x} - \int_2^x \frac{dt}{\log^2 t} \right).$$

Now

$$\begin{aligned} \int_2^x \frac{dt}{\log^2 t} &= \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \\ &\leq \frac{\sqrt{x}}{\log^2 2} + \frac{x - \sqrt{x}}{\log^2 \sqrt{x}} \\ &\leq \frac{\sqrt{x}}{\log^2 2} + \frac{x - \sqrt{x}}{\log^2 \sqrt{x}}. \end{aligned}$$

$$\text{Hence } \log x / x \int_2^x dt / \log^2 t \rightarrow 0.$$

This proves (7) \Rightarrow (6). So (6) and (7) are equivalent. Again (7) and (8) are equivalent. Hence we have (6) \Leftrightarrow (7) \Leftrightarrow (8). Hence proved.

THEOREM 4 : Let p_n denote the n^{th} prime then the following relations are equivalent:

$$(11) \lim_{x \rightarrow \infty} \pi(x) \log x / x = 1 \text{ and}$$

$$(12) \lim_{n \rightarrow \infty} p_n / n \log n = 1.$$

PROOF : To show (11) \Rightarrow (12).

Assume (11) holds. Taking logarithms we obtain

$$\lim_{x \rightarrow \infty} [\log \pi(x) + \log \log x - \log x] = 0$$

$$\Rightarrow \lim_{x \rightarrow \infty} [\log x (\log \pi(x) / \log x) + (\log \log x / \log x) - 1] = 0$$

$$\Rightarrow \lim_{x \rightarrow \infty} \log \pi(x) / \log x = 1.$$

So we get

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log \pi(x) \log x}{x \log x} = \lim_{x \rightarrow \infty} \left(\frac{\pi(x) \log x}{x} \right) \left(\frac{\log \pi(x)}{\log x} \right) = 1.$$

That is

$$\lim_{x \rightarrow \infty} \pi(x) \log \pi(x) / x = 1.$$

If $x = p_n$ then $\pi(x) = n$ and $\pi(x) \log \pi(x) = n \log n$

Hence, we get

$$\lim_{x \rightarrow \infty} \pi(x) \log \pi(x) / x = \lim_{x \rightarrow \infty} n \log n / p_n = 1.$$

Next to show that (12) \Rightarrow (11).

Assume (12) holds. Given x , define n by the inequalities

$$p_n \leq x < p_{n+1}$$

so that

$n = \pi(x)$. Dividing by $n \log n$, we get

$$\frac{p_n}{n \log n} \leq \frac{x}{n \log n} < \frac{p_{n+1}}{n \log n} = \frac{p_{n+1}}{(n+1) \log(n+1)} \frac{(n+1) \log(n+1)}{n \log n}.$$

Now let $n \rightarrow \infty$ and using (12) we get

$$\lim_{n \rightarrow \infty} x / n \log n = 1$$

$$\lim_{x \rightarrow \infty} x / \pi(x) \log \pi(x) = 1$$

or

$$(12) \lim_{x \rightarrow \infty} \pi(x) \log \pi(x) / x = 1.$$

Taking logarithm of both sides we obtain

$$\Rightarrow \lim_{x \rightarrow \infty} \log \left[\log \pi(x) \left(1 + \frac{\log \log \pi(x)}{\log \pi(x)} \right) \right] = 0.$$

Since $\log \pi(x) \rightarrow \infty$ as $x \rightarrow \infty$ it follows that

$$\lim_{x \rightarrow \infty} \left(1 + \frac{\log \log \pi(x)}{\log \pi(x)} - \frac{\log x}{\log \pi(x)} \right) = 0.$$

$$(13) \Rightarrow \lim_{x \rightarrow \infty} \log x / \log \pi(x) = 1$$

Now we get

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} &= \lim_{x \rightarrow \infty} \left[\frac{\pi(x) \log x}{x} \frac{\log x}{\log \pi(x)} \right] \\ &= \lim_{x \rightarrow \infty} \left(\frac{\pi(x) \log x}{x} \right) \lim_{x \rightarrow \infty} \left(\frac{\log x}{\log \pi(x)} \right) = 1. \end{aligned}$$

which proves (11) by (12) and (13).

4.4. INEQUALITIES FOR $\pi(n)$ AND p_n

THEOREM 5 : For every integer $n \geq 2$ we have

$$(14) \quad 1/6 \, n/\log n < \pi(n) < 6 \, n/\log n.$$

PROOF : Consider the binomial coefficient

$$\binom{2n}{n} = \frac{(2n)!}{n! n!}.$$

Now

$$4^n = (2^2)^n = 2^{2n} = (1+1)^{2n}$$

$$= \sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n}.$$

Also

$$2^n \leq \binom{2n}{n}.$$

For $n = 1$

$$2 = \binom{2}{1}.$$

For $n = 2$

$$2^2 = 4 < \binom{4}{2} = 4! / (2! 2!).$$

Assume it is true for n . To prove it for $(n+1)$

$$\begin{aligned} 2^{n+1} &= 2 \times 2^n \leq 2 \binom{2n}{2} = 2(2n)! / (n! n!) \\ &\leq \frac{2(n+1)(2n)!(n+1)}{n!(n+1)n!(n+1)} \\ &= \frac{(2n+1)(2n)!(2n+1)}{(n+1)!(n+1)!} \\ &\leq \frac{(2n+1)(2n)!(2n+1)}{(n+1)!(n+1)!} \\ &= \frac{(2n+2)!}{(n+1)!(n+1)!}. \end{aligned}$$

Hence $2^n \leq \binom{2n}{2}.$

is proved by induction on n , so we have

$$(15) \quad 2^n \leq \binom{2n}{2} < 4^n.$$

Taking logarithm of both sides of (15) we get

(16) $n \log 2 \leq \log (2n)! - 2 \log n! < n \log 4$. $\log (2n)!$ can be calculated from the Legendre's identity.

$$[x]! = \prod_{p \leq x} p^{\alpha(p)}$$

where $[x]$ is the greatest integer function.

This can be proved as follows :

$$\log[x]! = \sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d)$$

$$= \sum_{n \leq x} \Lambda(n) [x/n]$$

$$= \sum_{p \leq x} \sum_{m=1}^{\infty} [x/p^m] \log p$$

$$= \sum_{p \leq x} \alpha(p) \log p$$

where $\alpha(p) = \sum_{m=1}^{\infty} [x/p^m].$

Hence $\log n! = \sum_{p \leq n} \alpha(p) \log p$; where $\alpha(p) = \sum_{m=1}^{[\log n / \log p]} [n / p^m].$

Hence

$$\begin{aligned} & \log (2n)! - 2 \log n! \\ &= \sum_{p \leq 2n} \sum_{m=1}^{[\log 2n / \log p]} \{[2n/p^m] - 2[n/p^m]\} \log p. \end{aligned}$$

Since $[2x] - 2[x]$ is either 0 or 1,

(16) implies

$$n \log 2 \leq \sum_{p \leq 2n} \left(\sum_{m=1}^{[\log 2n / \log p]} 1 \right) \log p$$

$$\leq \sum_{p \leq 2n} \log 2n = \pi(2n) \log 2n.$$

This gives us

$$(17) \pi(2n) \geq \frac{n \log 2}{\log 2n} = \frac{2n}{\log 2n} \frac{\log 2}{12} > \frac{1}{4} \frac{2}{\log 2n}$$

since $\log 2 > 1/2$. For odd integers we have

$$(18) \pi(2n+1) \geq \pi(2n) >$$

$$\frac{1}{4} \frac{2n}{\log 2n} > \frac{1}{4} \frac{2n}{(2n+1) \log(2n+1)} \geq \frac{1}{6} \frac{(2n+1)}{\log(2n+1)}.$$

Since $2n / (2n+1) \geq 2/3$.

(17) and (18) imply

$$\pi(n) > 1/6 \quad n / \log n$$

for all $n \geq 2$ which proves left hand side of (14).

We will prove the right hand side inequality of (14).

$$\log(2n)! - 2 \log n! \geq \sum_{p \leq 2n} \{ [2n/p] - 2[n/p] \} \log p.$$

For primes p in the interval $n < p < 2n$, we have $[2n/p] - 2[n/p] = 1$

So

$$\log(2n)! - 2 \log n! \geq \sum_{n < p \leq 2n} \log p = \vartheta(2n) - \vartheta(n).$$

(16) implies

$$\vartheta(2n) - \vartheta(n) < n \log 4$$

If

$$n = 2^r \text{ then}$$

$$\vartheta(2^{r+1}) - \vartheta(2^r) < 2^r \log 4 = 2^{r+1} \log 2.$$

Summing on $r = 0, 1, 2, \dots, k$, we find

$$\vartheta(2^{k+1}) < 2^{k+2} \log 2.$$

Now we choose k so that $2^k \leq n < 2^{k+1}$, and we obtain

$$\vartheta(n) \leq \vartheta(2^{k+1}) < 2^{k+2} \log 2 \leq 4n \log 2$$

But if $0 < \alpha < 1$, we have

$$(\pi(n) - \pi(n^\alpha)) \log n^\alpha < \sum_{n^\alpha < p \leq n} \log p \leq \vartheta(n) < 4n \log 2.$$

$$\begin{aligned} \text{Hence } \pi(n) &< (4n \log 2 / \alpha \log n) + \pi(n^\alpha) < (4n \log 2 / \alpha \log n) + n^\alpha \\ &= n / \log n (4 \log 2 / \alpha + \log n / n^{1-\alpha}). \end{aligned}$$

Now if $c > 0$ and $n \geq 1$, the function $f(x) = x^{-c} \log x$ attains its maximum at $x = e^{1/c}$,

$$\text{so } n^{-c} \log n \leq 1/(ce) \text{ for } n \geq 1.$$

Taking $\alpha = 2/3$ in the inequality for $\pi(n)$ we find

$$\pi(n) < n/\log n (6 \log 2 + 3/e) < 6 (n/\log n).$$

This completes the proof.

4.5. PARTIAL SUMS OF MOBIUS FUNCTION

DEFINITIONS : If $x \geq 1$ we define

$$M(x) = \sum_{n \leq x} \mu(n).$$

The exact order of magnitude of $M(x)$ is not known. Numerical evidence suggests that

$$|M(x)| < \sqrt{x} \text{ if } x > 1.$$

Now we prove that the weaker statement

$$\lim_{x \rightarrow \infty} M(x) / x = 0$$

is equivalent to the prime number theorem. The behaviour of $\mu(x)$ as $x \rightarrow \infty$ is not so regular so we define another function $H(x)$ as follows:

DEFINITION : If $x \geq 1$ we define $H(x) = \sum_{n \leq x} \mu(n) \log n$.

This function $H(x)$ has relation with $\mu(x)$ which is obvious from the theorem.

THEOREM 6 : We have

$$(19) \lim_{x \rightarrow \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0.$$

$$\text{i.e. } \lim_{x \rightarrow \infty} \frac{M(x)}{x} = \lim_{x \rightarrow \infty} \frac{H(x)}{x \log x}.$$

PROOF : Taking $f(t) = \log t$ in theorem 2 with $y = 1$ we obtain

$$H(x) = \sum_{n \leq x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t} dt.$$

Hence if $x > 1$ we have,

$$\frac{M(x)}{x} - \frac{H(x)}{x \log x} = \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt.$$

Therefore to prove the theorem we must show that

$$(20) \quad \lim_{x \rightarrow \infty} \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt = 0.$$

From the definition of $M(x)$ it follows that $M(x) = O(x)$ so

$$\int_1^x \frac{M(t)}{t} dt = O\left(\int_1^x dt\right) = O(x)$$

Putting the value of the integral in (20) we get

$$\lim_{x \rightarrow \infty} \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt = \lim_{x \rightarrow \infty} \frac{O(x)}{x \log x} = 0.$$

Hence proved.

THEOREM 7 : The prime number theorem implies

$$\lim_{x \rightarrow \infty} \frac{M(x)}{x} = 0$$

PROOF : PNT $\Leftrightarrow \lim_{x \rightarrow \infty} \psi(x)/x = 1$ i.e. $\psi(x) \sim x$.

We know

$$\Lambda(n) = - \sum_{d|n} \mu(d) \log d$$

By Mobius inversion formula : The equation $f(n) = \sum_{d|n} g(d)$

$\Leftrightarrow g(n) = \sum_{d|n} f(d) \mu(n/d)$, we have

$$- \mu(n) \log n = \sum_{d|n} \mu(d) \Lambda(n/d)$$

$$\begin{aligned} \Rightarrow - \sum_{n \leq x} \mu(n) \log n &= \sum_{n \leq x} \sum_{d|n} \mu(d) \Lambda(n/d) \\ &= \sum_{n \leq x} \mu(n) \psi(x/n). \end{aligned}$$

(Since $\psi(x/n) = \sum_{k \leq x/n} \Lambda(k)$).

$$(21) \Rightarrow -H(x) = - \sum_{n \leq x} \mu(n) \log n = \sum_{n \leq x} \mu(n) \psi(x/n).$$

Since $\psi(x) \sim x$, if $\varepsilon > 0$ is given, there is a constant $A > 0$ such that

$$|\psi(x)/x - 1| < \varepsilon \text{ whenever } x \geq A.$$

$$\Rightarrow |\psi(x) - x| < \varepsilon x \text{ whenever } x \geq A.$$

Chose $x > A$ and splitting the sum on the right of (21) into two parts,

$$\sum_{n \leq y} + \sum_{y < n \leq x},$$

where $y = [x/A]$.

i.e.

$$\begin{aligned} \sum_{n \leq x} \mu(n) \psi(x/n) &= \sum_{n \leq y} \mu(n) \psi(x/n) + \sum_{y < n \leq x} \mu(n) \psi(x/n) \\ &= \Sigma_1 + \Sigma_2 \text{ say} \end{aligned}$$

Now

$$\begin{aligned} \Sigma_1 &= \sum_{n \leq y} \mu(n) \psi(x/n) = \sum_{n \leq y} \mu(n) (x/n + \psi(x/n) - x/n). \\ &= x \sum_{n \leq y} \mu(n)/n + \sum_{n \leq y} \mu(n) (\psi(x/n) - x/n) \end{aligned}$$

So

$$|\Sigma_1| = \left| \sum_{n \leq y} \mu(n) \psi(x/n) \right| \leq x \left| \sum_{n \leq y} \mu(n)/n \right|$$

$$+ \sum_{n \leq y} |\psi(x/n) - x/n|$$

$$< x + \varepsilon \sum_{n \leq y} x/n \quad (\text{Since } |\psi(x/n) - x/n| < \varepsilon x/n \text{ if } n \leq x/A = y)$$

$$< x + \varepsilon x (1 + \log y)$$

$$< x + \varepsilon x + \varepsilon x \log x.$$

In Σ_2 we have $y < n \leq x$ so $n \geq y + 1$

$$\text{Hence } x/n \leq x/y + 1 < A$$

$$\text{because } y \leq x/A < y + 1$$

$$x/n < A \Rightarrow \psi(x/n) \leq \psi(A).$$

$$|\Sigma_2| < x\psi(A)$$

$$\text{Hence } |H(x)| = \left| \sum_{n \leq x} \mu(n) \psi(x/n) \right| \leq |\Sigma_1| + |\Sigma_2|$$

$$< (1 + \varepsilon)x + \varepsilon x \log x + x\psi(A)$$

$$< (2 + \psi(A))x + \varepsilon x \log x \text{ if } \varepsilon < 1.$$

So given any ε such that $0 < \varepsilon < 1$ we have,

$$|H(x)| < (2 + \psi(A))x + \varepsilon x \log x \text{ if } x > A$$

$$\Rightarrow |H(x)| / x \log x < (2 + \psi(A)) / \log x + \varepsilon.$$

Choosing $B > A$ so that $x > B$ implies $(2 + \psi(A)) / \log x < \varepsilon$.

Then for $x > B$ we have

$$|H(x)| / x \log x < 2\varepsilon$$

$$\Rightarrow H(x) / (x \log x) \rightarrow 0 \text{ as } x \rightarrow \infty.$$

Hence proved.

The following gives the converse of theorem 7.

THEOREM 8 : $M(x) = o(x)$ as $x \rightarrow \infty$

$\Rightarrow \psi(x) \sim x$ as $x \rightarrow \infty$ i.e. PNT.

The proof is difficult. One can refer the book by Apostol (2).

THEOREM 9 : If

$$A(x) = \sum_{n \leq x} \mu(n)/n$$

the relation $A(x) = o(1)$ as $x \rightarrow \infty$ i.e. $A(x) \rightarrow 0$ as $x \rightarrow \infty$ implies PNT.

That is PNT is a consequence of the statement that the series $\sum_{n=1}^{\infty} \mu(n)/n$ is convergent to the sum 0.

PROOF : To prove the theorem we will show that $A(x) = o(1) \Rightarrow \mu(x) = o(x)$ which is equivalent to PNT. By Abel's identity we have

$$M(x) = \sum_{n \leq x} \mu(n) = \sum_{n \leq x} \mu(n)/n \cdot n$$

$$= x A(x) - \int_1^x A(t) dt$$

$$\Rightarrow M(x)/x = A(x) - 1/x \int_1^x A(t) dt$$

$$\Rightarrow \lim_{x \rightarrow \infty} M(x)/x = \lim_{x \rightarrow \infty} A(x) - \lim_{x \rightarrow \infty} 1/x \int_1^x A(t) dt.$$

In order to prove the theorem it is sufficient to show that

$$(22) \quad \lim_{x \rightarrow \infty} \frac{1}{x} \int_1^x A(t) dt = 0.$$

Since $A(x) = O(1)$ as $x \rightarrow \infty$, given $\varepsilon > 0$,

there exists s such that $|A(x)| < \varepsilon$ if $x \geq s$ and $|A(x)| \leq 1$ for all $x \geq 1$.

We have

$$\begin{aligned} \left| \frac{1}{x} \int_1^x A(t) dt \right| &\leq \left| \frac{1}{x} \int_1^s A(t) dt \right| + \left| \frac{1}{x} \int_s^x A(t) dt \right| \\ &\leq (s-1)/x + \varepsilon(x-s)/x. \end{aligned}$$

Letting $x \rightarrow \infty$ we find

$$\lim_{x \rightarrow \infty} \sup \left| \frac{1}{x} \int_1^x A(t) dt \right| \leq \varepsilon$$

and since ε is arbitrary this proves (22).

EXERCISE

1. Prove that the following two relations are equivalent ;
 (a) $\pi(x) = x / \log x + O(x / \log^2 x)$
 (b) $\vartheta(x) = x + O(x / \log x)$.
2. If $a > 0$ and $b > 0$ then prove that
 $\pi(ax) / \pi(bx) \sim a/b$ as $x \rightarrow \infty$.
3. If $0 < a < b$, there exists an x_0 such that $\pi(ax) < \pi(bx)$ if $x \geq x_0$.
4. Prove that for every $n > 1$ there exists n consecutive composite numbers.
5. Let S_n denote the sum of first n primes. Prove that for each n there exists an integer whose square lies between S_n and S_{n+1} .
6. Let S_n denote the n^{th} partial sum of the series $\sum_{r=1}^{\infty} 1 / r(r+1)$.
 prove that for every integer $k > 1$ there exists m and n such that $S_m - S_n = 1/k$.
7. Prove that for all $x \geq 1$ we have $\sum_{n \leq x} \Lambda(n) / n = \log x + O(1)$.



CRYPTOGRAPHY

BASIC NOTIONS : Cryptography is the study of method of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plaintext and the disguised message is called the ciphertext. The plaintext and ciphertext are written in some alphabet consisting of certain number N of letters. The term "letter" (or "character") can refer not only to the families A–Z, but also to numerals blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages. The process of converting a plaintext to a ciphertext is called enciphering or encryption, and the reverse process is called deciphering.

The plaintext and ciphertext are broken up into message units. A message unit might be a single letter, or pair of letters (digraph), a triple of letters (trigraph), or block of 50 letters. An enciphering transformation is a function from plaintext message unit to ciphertext message unit i.e. $f: P \rightarrow C$.

The deciphering transformation is the map f^{-1} which recovers the plaintext from the ciphertext i.e. $C \xrightarrow{f^{-1}} P$.

So

$$(1) \quad P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

Such a set up is called cryptosystem.

5.1. CLASSICAL CRYPTOSYSTEM :

Classically, the making and breaking of secret codes has usually been confined to diplomatic and military practices. With the growing quantity of digital data stored and communicated by electronic data processing systems,

organization in both public and commercial sectors have felt the need to protect information from unwanted intrusion .

One of the earliest cryptographic system was used by the great Roman emperor Julius Caesar around 50 BC Caesar wrote to Marcus Cicero using a rudimentary substitution cipher in which each letter of alphabet is replaced by the letter which occurs three places down the alphabet, with the last three letters cycled back to the first three letters. thus Caesar Cipher is given by

(2) P: ABCDEFGHIJKLMNOPQRSTUVWXYZ

C: DEFGHIJKLMNOPQRSTUVWXYZ ABC

Example : Plaintext message P is

(3) CAESAR WAS GREAT

is transformed into ciphertext message i.e. by Caesar cipher (2)

(4) FDHVDU ZDV JUHDV.

The Caesar cipher can be described only using congruence theory .

We first give numerical values to the alphabets A–Z as follow.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Some authors assign values 0–25 to A – Z. One should follow one of these two sets of values.

If P is the digital equivalent of a plaintext letter and C is the digital equivalent of the corresponding ciphertext letter, then

$$C \equiv P + 3 \pmod{26}.$$

Thus the letter of the message (3) are converted to the equivalents :

(5) 01 05 19 01 18 23 01 19 07 18 05 01 20. Using the congruence

$$C \equiv P+3 \pmod{26},$$

this becomes the ciphertext.

(6) 06 04 08 22 04 21 26 04 22 10 21 08 04 23.

To recover the plaintext, the procedure is

$$P \equiv C - 3 \equiv C + 23 \pmod{26}.$$

That is given ciphertext if we add 23 to each of the numerical values and reduce it to modulo 26 we get the numerical equivalent of the plaintext and

That is given ciphertext if we add 23 to each of the numerical values and reduce it to modulo 26 we get the numerical equivalent of the plaintext and thus read the message.

The Caesar cipher is simple and hence insecure .

In conventional Cryptosystem, the sender and receiver jointly have a secret key. The sender uses the key to encrypt the plaintext to be sent, while the receiver uses the same key in order to decrypt the ciphertext obtained. Public key cryptography differs from conventional cryptography in that it uses two keys, an enciphering key K_E and the deciphering key K_D . Cryptoanalysis is the science of decoding the ciphertext without the knowledge of the key.

Example 1 : Suppose we are using 26 letter alphabets A–Z with numerical equivalents 0–25.

Let the letter $P \in \{ 0, 1, \dots, 25 \}$ stands for a plaintext message unit.

Define $f : P \rightarrow C$

$$f(P) = \begin{cases} P+3 & \text{if } x < 23 \\ P-23 & \text{if } x \geq 23. \end{cases}$$

i.e. $f(P) = P + 3 \pmod{26}$

In general we write

$$C = f(P) \equiv P + b \pmod{N}.$$

where b is a fixed integer which is the letter alphabet with numerical equivalents 0, 1, 2, ..., $N-1$. To decipher the ciphertext message unit $C \in \{ 0, 1, 2, \dots, N-1 \}$,

we compute

$$P = f^{-1}(C) = C - b \pmod{N}$$

and b is called is key and call f a shift transformation .

As a special case we have Caesar cipher with $N = 26$ and $b = 3$. Suppose we want to encipher the word "Book". We first convert to numbers.

01 14 14 10,

then add 3 modulo 26, This transforms to

04 17 17 13,

then translate back to letters "ERRN".

To decipher the message one subtract 3 mod 26. For example the ciphertext "ZKB" gives the plaintext "WHY".

Example 2 : (Frequency Analysis)

Suppose we intercept a message which we know was enciphered using a shift transformation on single letter of the 26-letter alphabet, we have to find b . For this we use frequency analysis which means the frequently occurring letter in the English language. We note that "E" is the most frequently occurring letter in the English language so it is reasonable to assume that the most frequently occurring letter in ciphertext is the encryption of E.

Suppose the ciphertext message is "PXCDEXFXDPRA". "X" is the most frequently occurring character in the ciphertext. That means the shift takes "E" = 4 to "X" = 23 i.e. $23 \equiv 4 + b \pmod{26}$, so that $b = 19$ to decipher the message, hen, it remains to subtract 19 from the numerical equivalents of

"PXCDEXFXDPRA"

" PXCDEXFXDPRA" = 15 23 02 03 04 23 05 23 03 15 17 0

→ 22 04 09 10 11 04 12 04 10 22 24 7

= "WE JKLEMEKWHYH"

[Since $-19 \equiv 7 \pmod{26}$ we add 7 mod 26]

Example 3 : If we encipher the ciphertext "FQOCUDEM" assuming 'U' as the frequently occurring character in the ciphertext then the message is "PAYMENOW".

AFFINE TRANSFORMATION : This is a more general type of transformation of (Z/NZ) called an affine map.

$C = aP + b \pmod{N}$, where a and b are fixed integers they together form the enciphering key $K_E = (a, b)$.

To decipher a message that was enciphered by means of the affn map

$C \equiv aP + b \pmod{N}$ to solve for $P \equiv a^{-1} C + b^{-1} \pmod{N}$ where a^{-1} is the inverse of $a \pmod{N}$ and b is equal to $-a^{-1} b$. This works only if $\text{g.c.d.}(a, N) = 1$. The deciphering key K_D is the pair (a^{-1}, b^{-1}) .

Example 4 : Suppose a ciphertext is given written in 26-letter alphabet with A–Z assigned the numerical values 0–25. Suppose we know most frequently occurring letter of ciphertext is "K", and the second most frequently occurring letter is "D". It is reasonable to assume that these are the encryption of "E" and "T" respectively, which are the two most frequently occurring letters in the English language. thus replacing the letter by their numerical equivalents and substituting for P and C in the deciphering formula we get

$$10a' + b' \equiv 4 \pmod{26}$$

$$3a' + b' \equiv 19 \pmod{26}.$$

Since "E" = 4 "D" = 3 "T" = 19 and "K" = 10.

We have to solve the congruence for a' and b' subtracting we get

$$7a' \equiv 11 \pmod{26}$$

and

$$a' \equiv 7^{-1} \cdot 11.$$

Since

$$7 \cdot 7^{-1} \equiv 1 \pmod{26} \Rightarrow 7^{-1} = 15$$

since

$$7 \cdot 15 \equiv 1 \pmod{26}.$$

Hence

$$a' \equiv 7^{-1} \cdot 11 \equiv 15 \cdot 11 \equiv 165 \equiv 9 \pmod{26}$$

By putting the value of a' in the first congruence we get

$$10 \times 9 + b' \equiv 4 \pmod{26}$$

\Rightarrow

$$b' \equiv 4 - 90 \pmod{26} \equiv 18 \pmod{26}$$

So the message can be deciphered by means of the formula

$$P \equiv 9C + 18 \pmod{26}.$$

DIGRAPH : If our message units are digraphs in 27 letter alphabet consisting of A–Z and a blank, we might first let the blank have numerical equivalent 26 and then label the digraph whose two letters corresponding to $x, y \in \{0, 1, 2, \dots, 26\}$. By the integer

$$27x + y \in \{0, 1, 2, \dots, 728\}.$$

We consider the individual letters as digits to the base 27 and we view the digraph as a 2-digit integer to that base.

Example 1 : The digraph "No" corresponds to the integer

$$27 \cdot 13 + 14 = 365$$

since

$$N = 13 \text{ and } 0 = 14.$$

TRIGRAPH : If we use trigraphs as our message units, we could label them by integer

$$27^2 x + 27 y + z \in \{0, 1, \dots, 27^3 - 1 = 19682\}.$$

In general, we can label blocks of k letters in an N -letter alphabet by integers between 0 and $N^k - 1$ by regarding each block as a k -digit integer to the base N .

5.2. PUBLIC KEY CRYPTOGRAPHY

We studied in 5.1 that a cryptosystem consist of a 1to 1 transformation f :

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

We use enciphering key K_E is the pair (a,b) and deciphering key K_D to compute f^{-1} .

In affine cryptosystem family, deciphering is accomplished by an affine map, namely

$$P \equiv a^{-1} C - a^{-1} b \pmod{N}.$$

Here one would have to allow the possibility of examining a large number of corresponding plaintext ciphertext message units because by the definition of public key system, any user can generate an arbitrary number of plaintext – ciphertext pairs.

The name “public key” means that the information needed to send secret message the enciphering key K_E can be made public information without enabling any one to read the secret message.

Suppose we have some population of users of the cryptosystem, each one of whom wants to be able to receive confidential communications from any one of the other users without a third party being able to decipher the message. Some central office can collect the enciphering key $K_{E,A}$ from each user A and publish all of the keys in a “telephone book”. Some one wanting to send a message merely has to look up the enciphering key in this “telephone book” and then use the general enciphering algorithm with the key parameters corresponding to the intended recipient. Only the intended recipient has the matching deciphering key needed to read the message.

We notice that with a public key system it is possible for two parties to initiate secret communication without ever having had any prior contact without having established any prior trust for one another, without exchanging any preliminary information. The information necessary is publicly available. To decipher the message it is not always easy for the public to get the deciphering key.

DEFINITION : We define, a public key cryptosystem is a system with the property that some one who knows only how to encipher can not use the enciphering key to find the deciphering key without a prohibitively lengthy computation.

In other words the enciphering function $f : P \rightarrow C$ is easy to compute once the enciphering K_E is known, but it is very hard to compute the inverse function

$f^{-1} : C \rightarrow P$. That is the function f is not invertible without some additional information. Such a function f is called a one-way function or a trapdoor function.

COMPARISON OF CLASSICAL CRYPTOSYSTEM AND PUBLIC KEY CRYPTOSYSTEM .

Classical Crypto system	Public key Crypto system
<ol style="list-style-type: none"> 1. Once enciphering information is known, the deciphering information can be implemented in approximately same order of magnitude of as the enciphering transformation. 2. It takes a little longer time for decipher because one needs to apply Euclidean algorithm to find an inverse modulo N. 3. The authentication of the communication is not maintained. 4. In this system sending message is faster to implement. 5. Lacks in integrity. 6. The number of plaintext message units per second that can be transmitted is more. 7. It is widely put to use . 8. Message would be sent faster 	<ol style="list-style-type: none"> 1. Once enciphering key K_E is known it is hard to find the deciphering key K_D to decipher, the message. 2. Time required is less in comparison to classical cryptosystem. 3. The authentication of the communication is maintained. The signature of the message known to the persons can read the message. 4. In this system for sending message tend to be slower to implement. 5. It has integrity i.e. the recipient of a message should be able to determine that the message has not been modified in transit. 6. The number of plaintext message unit per second that can be transmitted is less. 7. It is not widely put to use. 8. Message would not be sent faster.

Public key cryptography has found numerous applications:

1. Paper documents such as checks, stocks, lottery tickets can be authenticated using public key techniques. A document is assigned a unique digital signature based on fiber patterns of the paper and the contents of the document. The signature is encoded with a private key and the resulting cipher is affixed to the document. Any one can verify the authenticity of the document by using an embedded public key.

2. Public key techniques are now used in smart card, digital cash other types of electronic banking and commerce .

5.3. THE RSA CRYPTOSYSTEM

The RSA cryptosystem is one of the most popular public-key cryptosystem. It was invented by R.L. Rivest, A. Shamir and L.M. Adleman in 1978 The success of "RSA" cryptosystem and most popular public key cryptosystem , is based on the tremendous difficulty of factoring.

We now describe how RSA works. Each user first choose two extremely large prime numbers p and q and set $n = pq$, knowing the factorization of n , it is easy to compute $\phi(n) = (p-1)(q-1) = pq + 1 - p - q = n + 1 - p - q$. Next , the user randomly choose an integer e between 1 and $\phi(n)$ such that $\gcd(e, \phi(n)) = 1$. Thus each user A chooses two primes P_A and Q_A and a random number e_A which has no common factor with $(p_A-1)(q_A-1)$. Next , A computes $n_A = p_A q_A$, $\phi(n_A) = n_A + 1 - p_A - q_A$ and the multiplication inverse of e_A modulo $\phi(n_A)$. $d_A \text{ def. } \equiv e_A^{-1} \pmod{\phi(n_A)}$. Then make public and is placed in telephone directory the enciphering key $K_{E,A} = (n_A, e_A)$ and conceals the deciphering key $K_{D,A} = (n_A, d_A)$. Notice that when n_A is openly revealed, the listed public key does not mention the factors p_A and q_A of n_A .

The enciphering transformation is the map

$$f : Z/n_A Z \rightarrow Z/n_A Z \text{ given by } f(P) = P^{e_A} \pmod{n_A}.$$

The deciphering transformation is the map f from $Z/n_A Z$ to it self given by

$$f(C) = C^{d_A} \pmod{n_A}.$$

f and f^{-1} are inverse of each other because of our choice of d_A .

To work with it is assumed that the plaintext number $M < n_A$, where n_A is the enciphering modulus . If the message is too length to be handled as a single number $M < n_A$, then M can be broken up into blocks of digits M_1, M_2, \dots, M_r of the appropriate size . Each block would be encrypted separately. We will illustrate RSA system by means of example.

Example 1 : Let us choose $N = 26$, Let the plaintext consists of trigraphs and ciphertext consist of four-graphs in the usual 26 letter alphabet. we want to send the message "YES" to a user A with enciphering key $(n_A, e_A) = (46927, 39423)$, we first find numerical equivalent of "YES" i.e. $Y = 24, E = 4, S = 18$ $24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346$ and then compute

$$P^{e_A} \pmod{m} = 16346^{39423} \pmod{46927}$$

which is $21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 5 \cdot 26 + 2 = \text{"BFIC"}$.

To decipher the message the recipient knows the deciphering key

$$(n_A, d_A) = (46927, 26767) = 26767 \text{ and so compute}$$

$$\begin{aligned} C^{d_A} \pmod{n_A} &= 21166 \pmod{46927} = 16346 \\ &= 24.26^2 + 4.26 + 18 = \text{"YES"}. \end{aligned}$$

The user A generates his key like this first he multiplies the primes $P_A = 281$ and $Q_A = 167$ to get n_A . Then he chooses e_A at random so that

$$\gcd(e_A, \phi(n_A)) = 1.$$

Then he chooses d_A such that $e_A d_A \equiv 1 \pmod{\phi(n_A)}$. The number p_A, q_A, d_A remain secret.

Example 2 : To encrypt the message "NO WAY" by RSA system.

First select two small primes $p=29, q=53$. Then our enciphering modulus

$$n = pq = 29.53 = 1537,$$

$$\phi(n) = 28.52 = 1457$$

choose the exponent $e = 47$ such that

$$\gcd(47, 1457) = 1.$$

Find the inverse of e i.e. $e^{-1} = d$ such that

$$e \cdot d \equiv 1 \pmod{1457}$$

$$\text{i.e. } 47 \cdot d \equiv 1 \pmod{1457}$$

$$\Rightarrow d = 31.$$

Now to encrypt the message $M = \text{"NO WAY"}$.

The numerical equivalent of plaintext M in 26 – letter alphabet A–Z with numerical equivalent (1 to 26) $M = 141500230125$.

As M is large split M into blocks of three digits. The first block, 141, encrypt as the ciphertext number $141^{47} \equiv 658 \pmod{1537}$ on the other hand knowing the recovery exponent $d = 31$ the recipient would begin to recover the first block of the plaintext number $658^{31} \equiv 141 \pmod{1537}$. The total ciphertext of our message M is 0658 1408 1250 1252.

Remark : This method is most secure in the sense that it is not feasible to recover the plaintext M from the information assumed to be known to a third party, the listed public-key (n_A, e_A) . The method is to factorize n_A (huge number) then d can be calculated from $\phi(n_A) = (p_A - 1)(q_A - 1)$ and e_A . Factoring a large number is very difficult even in computer.

There are other methods of public key cryptography. They are

1. Discrete log method
2. The ElGamal cryptosystem.
3. The Massey–Omura cryptosystem.
4. The knapsack problem we are not discussing in the present text. However in the last chapter as application we will study Discrete log method and the ElGamal crypto system.

EXERCISES

1. Encrypt the message "NUMBER THEORY" using Caesar cipher.
2. Using the linear cipher $C \equiv 5p + 11 \pmod{26}$, encrypt the message "READ NUMBER THEORY".
3. If $n = pq = 274279$ and $\phi(n) = 272376$, find prime p and q .
4. If the enciphering key in a RSA system $(n, e) = (3233, 37)$. Find the recovery exponent.
5. Decipher the message TZSVIW JQBVMIJ AL MVOOVI; which was produced using the cipher $C \equiv 3p + 7 \pmod{26}$.
6. Suppose that $n = 10088821$ is a product of two distinct primes, and $\phi(n) = 10082272$. Determine the prime factor of n .
Hints: $p + q = n - \phi(n) + 1$
 $p - q = [(p+q)^2 - 4n]^{1/2}$.
7. If the modulus in RSA system is $n = 1146115723$ and encrypting key $e = 67$, compute the deciphering key and decrypt the following cipher and recover the plaintext. 474786165, 121618407.



PRIMITIVE ROOTS AND INDICES

6.1. PRIMITIVE ROOTS

We define the order, primitive roots of an integer modulo n which has application in cryptography specially in primality testing.

DEFINITION 1 : Let a and n be integers such that $(a, n) = 1$. Then the order of a modulo n , denoted by $\text{ord}_n(a)$ is the smallest positive integer k such that

$$(1) \quad a^k \equiv 1 \pmod{n}.$$

Example 1 : The order of 3 modulo 5 is 4.

we have $3 \equiv 3 \pmod{5}$

$$3^2 \equiv 4 \pmod{5}$$

$$3^3 \equiv 2 \pmod{5}$$

$$3^4 \equiv 1 \pmod{5}.$$

Example 2 : The order of 2 mod 17 is 8 and the order of 5 mod 19 is 9.

$$2 \equiv 2 \pmod{17}$$

$$2^2 \equiv 4 \pmod{17}$$

$$2^3 \equiv 8 \pmod{17}$$

$$2^4 \equiv 16 \pmod{17}$$

$$2^5 \equiv 15 \pmod{17}$$

$$2^6 \equiv 13 \pmod{17}$$

$$2^7 \equiv 9 \pmod{17}$$

$$2^8 \equiv 1 \pmod{17}$$

$$5 \equiv 5 \pmod{19}$$

$$5^2 \equiv 9 \pmod{19}$$

$$5^3 \equiv 11 \pmod{19}$$

$$5^4 \equiv 17 \pmod{19}$$

$$5^5 \equiv 16 \pmod{19}$$

$$5^6 \equiv 7 \pmod{19}$$

$$5^7 \equiv 16 \pmod{19}$$

$$5^8 \equiv 4 \pmod{19}$$

$$5^9 \equiv 1 \pmod{19}.$$

THEOREM 1 : Given $n \geq 1$ and $(a, n) = 1$. If a has order k modulo n then

(i) $a^i \equiv a^j \pmod{n}$, if, and only if $i \equiv j \pmod{k}$.

(ii) $a^i \equiv 1 \pmod{n}$, if and only if $i \equiv 0 \pmod{k}$ that is $k \mid i$.

In particular $k \mid \phi(n)$.

PROOF OF THE THEOREM : We will first prove (i). If $a^i \equiv a^j \pmod{n}$, then $a^{i-j} \equiv 1 \pmod{n}$ by Euclidean algorithm we write.

$$i-j = qk + r, \text{ where } 0 \leq r < k.$$

Then $1 \equiv a^{i-j} = a^{qk+r} \equiv a^r \pmod{n}$ since a has order k .

So, $r = 0$ and $i \equiv j \pmod{k}$.

Conversely if $i \equiv j \pmod{k}$ then $i - j = qk$.

So $a^{i-j} \equiv a^{qk} \equiv (a^k)^q \equiv 1 \pmod{n}$

Hence $a^i \equiv a^j \pmod{n}$.

Proof of (iii) follows from (i).

Proof of (ii) If $a^i \equiv 1 \pmod{n}$ then $i \geq k$. because k is the order a modulo n , we write

$$i = kq + r, 0 \leq r < k.$$

Now $a^i = a^{kq+r} = a^{kq} a^r = (a^k)^q a^r$
 $\equiv 1^q a^r \equiv a^r \pmod{n}$.

So $a^i \equiv 1 \pmod{n}$ implies that $a^r \equiv 1 \pmod{n}$

which is impossible since $0 \leq r < k$

Hence $r = 0$ i.e. $i = kq$.

Hence $k \mid i$.

Conversely if $i \equiv 0 \pmod{k}$ i.e. $k \mid i$ we write $i = kq$. Then we get

$$a^i = a^{kq} = (a^k)^q \equiv 1 \pmod{n}.$$

By Euler -Fermat's theorem we know, if $(a, n) = 1$,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

By (ii) it follow that $k \mid \phi(n)$. Since k is the order r of a modulo n . Hence proved.

THEOREM 2 : If the integer a has order k modulo n and $h > 0$. then a^h has order

$$k / \gcd(h, k).$$

PROOF : Let $d = \gcd(h, k)$. Then we write $h = h_1 d$ and $k = k_1 d$ with $\gcd(h_1, k_1) = 1$.

Clearly

$$(a^h)^{k_1} = (a^{h_1 d})^{k_1} = (a^k)^{h_1} \equiv 1 \pmod{n}.$$

If a^h is assumed to have order $r \bmod n$, then we have $r|k_1$. On the other hand, since a has order $k \bmod n$, the congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

implies that $k|hr$, in other words $k_1d | h_1dr$ or $k_1 | h_1r$. But $\gcd(h_1, k_1) = 1$ and therefore $k_1|r$. This gives

$$r = k_1 = k/d = k / \gcd(h, k).$$

This completes the proof of the theorem.

Corollary : Let a has order k modulo n . Then a^h also has order k if and only if

$$\gcd(h, k) = 1.$$

The proof follows directly from the above theorem by taking $d = 1$.

DEFINITION 2 : (Primitive Root) If the order of $a \bmod n$ is $\Phi(n)$ then a is called a primitive root of n or a primitive root modulo n .

The statement that a is a primitive root of n implies the following :

$$(a) (a, n) = 1$$

$$(b) a^{\Phi(n)} \equiv 1 \pmod{n}$$

$$(c) a^h \equiv 1 \pmod{n}, 0 < h < \Phi(n).$$

Conversely (a), (b), (c) imply that a is a primitive root of n . It follows from the definition.

Example 1 : Show that 2 is a primitive root of 11.

Solution : If $a^d \equiv 1 \pmod{n}$ then d divides $\phi(11)$. The divisor of $\phi(11) = 10$ are 2, 5 and 10.

We then find

$$2^2 \equiv 4 \pmod{11}$$

$$2^5 \equiv -1 \pmod{11}$$

$$2^{10} \equiv 1 \pmod{11}.$$

So the smallest integer x which satisfies $2^x \equiv 1 \pmod{11}$ is 10. This implies 2 is a primitive root of modulo 11.

Example 2 : Show that 5 is a primitive root of 18.

Solution : $\phi(18) = 6 = 2 \times 3$. Hence the divisors of $\phi(18)$ are 2, 3, and 6.

Now

$$5^2 \equiv 7 \pmod{18}, 5^3 \equiv -1 \pmod{18}, 5^6 \equiv 1 \pmod{18}$$

It follow that 5 is a primitive root of 18.

THEOREM 3 : Let $(a, n) = 1$ then a is a primitive root of n if and only if

$$(2) a^{\phi(n)/p} \not\equiv 1 \pmod{n}$$

for every prime divisor p of $\phi(n)$.

PROOF : Let a be such that (2) holds i.e.

$$a^{\phi(n)/p} \not\equiv 1 \pmod{p}$$

for every prime divisor p of $\phi(n)$. Let us assume that under this condition a is not a primitive root of n . Then it follows that the order of a is some integer k less than $\phi(n)$. This implies that k divides $\phi(n)$. Thus $\phi(n)/k$ is an integer and is therefore divided by some prime divisor p of $\phi(n)$.

Hence

$$a^{\phi(n)/p} = (a^k)^{\phi(n)/kp} \equiv 1 \pmod{n}$$

because $a^k \equiv 1 \pmod{n}$. This contradicts (2) alone.

Let a be a primitive root of n . Then it follows that

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ and } a^h \not\equiv 1 \pmod{n}.$$

This means that $a^{\phi(n)/p} \not\equiv 1 \pmod{n}$ for every prime divisor p of $\phi(n)$.

Example 1 : Find all primitive roots of 19.

Solution : $\phi(19) = 18 = 2 \times 3^2$. So 2, 3 are only prime divisors of $\phi(n)$. But

$$\frac{\phi(19)}{3} = \frac{18}{3} = 6 \text{ and } \frac{\phi(19)}{2} = \frac{18}{2} = 9.$$

So, a is a primitive root of 19 if and only if $a^6 \not\equiv 1 \pmod{19}$ and $a^9 \not\equiv 1 \pmod{19}$. Letting $a = 2, 3, \dots, 18$ in succession we find the following modulo 19.

$2^6 \equiv 7$	$2^9 \equiv -1$	Primitive root
$3^6 \equiv 7$	$3^9 \equiv -1$	Primitive root
$4^6 \equiv 11$	$4^9 \equiv 1$	
$5^6 \equiv 7$	$5^9 \equiv 1$	
$6^6 \equiv 11$	$6^9 \equiv 1$	
$7^6 \equiv 1$	$7^9 \equiv 1$	
$8^6 \equiv 1$	$8^9 \equiv -1$	
$9^6 \equiv 11$	$9^9 \equiv 1$	
$10^6 \equiv 11$	$10^9 \equiv -1$	Primitive root
$11^6 \equiv 1$	$11^9 \equiv 1$	

$12^6 \equiv 1$	$12^9 \equiv -1$	
$13^6 \equiv 11$	$13^9 \equiv -1$	Primitive root
$14^6 \equiv 7$	$14^9 \equiv -1$	Primitive root
$15^6 \equiv 11$	$15^9 \equiv -1$	Primitive root
$16^6 \equiv 7$	$16^9 \equiv 1$	
$17^6 \equiv 7$	$17^9 \equiv 1$	
$18^6 \equiv 1$	$18^9 \equiv -1$	

It follows that 2, 3, 10, 13, 14 and 15 are primitive roots modulo 19.

Exercise : Find all primitive roots of 15, 17.

Example 2 : If $F_n = 2^{2^n} + 1$, $n > 1$ is a prime, then 2 is not a primitive root of F_n .

Solution : Since $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$

we have $2^{2^{n+1}} \equiv 1 \pmod{F_n}$

which implies that the order of 2 modulo F_n does not exceed 2^{n+1} . But if F_n is assumed to be prime,

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

and since $2^{2^n} > 2^{n+1}$, whenever $n > 1$.

Thus the order of 2 modulo F_n is smaller than $\phi(F_n)$; ie 2 can not be a primitive root of F_n .

But 2 is a primitive root $5 = F_1$.

THEOREM 4 : Let $\gcd(a, n) = 1$ and let $a_1, a_2, \dots, a_{\phi(n)}$ be the positive integer less than n and relatively prime to n . If a is a primitive root of n , then $a, a^2, \dots, a^{\phi(n)}$ are congruent modulo n to $a_1, a_2, \dots, a_{\phi(n)}$ in some order.

PROOF : Since $(a, n) = 1$ the same is true for all powers of a ; hence,

each $a^k \equiv a_l \pmod{n}$. The $\phi(n)$ numbers in the set $\{a, a^2, \dots, a^{\phi(n)}\}$ are incongruent modulo n . Hence these powers must represent the integer $a_1, a_2, \dots, a_{\phi(n)}$.

Corollary 1 : If n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

PROOF : Suppose that a is a primitive root of n . By the theorem, any other primitive root of n is found among member of the set $\{a, a^2, \dots, a^{\phi(n)}\}$. But the number of powers a^k , $1 \leq k \leq \phi(n)$ which have order $\phi(n)$ is equal to the number of integer k for which $\gcd(k, \phi(n)) = 1$; there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n .

Example : Take $a = 2$ and $n = 9$, then

$\phi(9) = 6$, the first 6 powers of 2 i.e. $2, 2^2, 2^3, 2^4, 2^5, 2^6$ must be congruent modulo 9, in some order to the positive integers less than 9 and relatively prime to it. These integers less than 9 and relatively prime to 9 are 1, 2, 4, 5, 7, 8 and

$$2^1 \equiv 2 \pmod{9}$$

$$2^2 \equiv 4 \pmod{9}$$

$$2^3 \equiv 8 \pmod{9}$$

$$2^4 \equiv 7 \pmod{9}$$

$$2^5 \equiv 5 \pmod{9}$$

$$2^6 \equiv 1 \pmod{9}.$$

There are $\phi(\phi(9)) = \phi(6) = 2$, primitive roots of 9. These are the integers 2 and 5.

THEOREM 5 : Let a be a primitive root of n and let $a_1 \equiv a \pmod{n}$. Then a_1 is also a primitive root of n .

PROOF : The order of $a \pmod{n}$ is $\phi(n)$. Hence the order of $a_1 \pmod{n}$ is $\phi(n)$. This implies that a_1 is a primitive root of n . Hence proved.

6.2. REDUCED RESIDUE SYSTEM.

THEOREM 6 : Let $(a, n) = 1$. Then a is a primitive root modulo n if, and only if the numbers

$$(3) \ a, a^2, \dots, a^{\phi(n)}$$

form a reduced residue system modulo n .

PROOF : If a is a primitive root of n the number in (3) are incongruent modulo n since there are $\phi(n)$ such numbers they form a reduced system modulo n .

Conversely, if the numbers in (3) form a reduced residue system, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

But no smaller power is congruent to 1, so a is a primitive root. Hence proved.

If n has a primitive root then each reduced residue system modulo n can be expressed as a geometric progression. But the primitive root exists only for the following modulo:

$$n = 1, 2, 2^2, p^k \text{ and } 2p^k$$

where p is an odd prime and $k \geq 1$.

The case $n = 1$ is trivial For $n = 2$, the number 1 is a primitive root.

For $n = 4$, $\phi(4) = 2$ and $3^2 = 1 \pmod{4}$, so 3 is a primitive root $\pmod{4}$. We will show that there are now primitive root modulo 2^k if $k \geq 3$.

THEOREM 7 : For $k \geq 3$, the integer 2^k has no primitive root.

PROOF : To show that if a is an odd integer, then for $k \geq 3$

$$(4) \quad a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

If $k = 3$, (4) becomes

$$a^2 \equiv 1 \pmod{8} \text{ which is true for } a = 1, 3, 5, 7.$$

Assume that (4) holds for integer k , i.e. $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ equivalently

$$a^{2^{k-2}} \equiv 1 + m 2^k \text{ where } m \text{ is an integer.}$$

Squaring both sides we get

$$\begin{aligned} a^{2^{k-1}} &= (a^{2^{k-2}})^2 = (1 + m 2^k)^2 \\ &= 1 + 2(m 2^k) + (m 2^k)^2 \\ &= 1 + 2^{k+1}(m + m^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}} \end{aligned}$$

So (4) holds for $k+1$ and hence for all $k \geq 3$.

Now the integers which are relative prime to 2^k are the odd integer; also

$$\phi(2^k) = 2^{k-1}. \text{ If } a \text{ is an odd integer and } k \geq 3,$$

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$$

and, consequently there are no primitive roots of 2^k .

THEOREM 8 : If $\gcd(m, n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive root.

PROOF : Consider any integer a for which $(a, mn) = 1$, then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$, put $h = \text{lcm}(\phi(m), \phi(n))$ and $d = \gcd(\phi(m), \phi(n))$.

Since $\phi(m)$ and $\phi(n)$ are both even, $d \geq 2$.

$$h = \frac{\phi(m) \phi(n)}{d} \leq \frac{\phi(mn)}{2} \left(\text{Since } \text{lcm}(a, b) = \frac{ab}{\gcd(a, b)} \right)$$

By Euler's Theorem $a^{\phi(m)} \equiv 1 \pmod{m}$

$$\begin{aligned} a^h &= (a^{\phi(m)})^{\phi(n)/d} \equiv (1)^{\phi(n)/d} \\ &\equiv 1 \pmod{m}. \end{aligned}$$

Similarly $a^h \equiv 1 \pmod{n}$.

Since $\gcd(m, n) = 1$ These two imply that

$$a^h \equiv 1 \pmod{mn}.$$

Hence there can be no primitive root of mn .

6.3. PRIMITIVE ROOTS MODULO PRIME

We now determine all integers that have primitive roots belonging to them. We prove the following theorem.

THEOREM 9 : There exists at least one primitive root modulo each prime $p \geq 3$.

PROOF : Let p be a prime ≥ 3 . To find integer that have order $\phi(p) = p-1 \pmod{p}$.

If a is any integer having order $n \pmod{p}$, then $(a, p) = 1$, implies

$$a^{p-1} \equiv 1 \pmod{p} \text{ (Fermat's Theorem) Hence } n \mid p-1.$$

Conversely, for any divisor m of $p-1$ the polynomial congruence

$$(5) \ x^m \equiv 1 \pmod{p}$$

has at most m mutually incongruent solutions. Let b be an integer having order $m \pmod{p}$. Then b is a solution of (5). In fact, $1, b, b^2, \dots, b^{m-1}$ are all the solutions of (5) (modulo p).

The congruence (5) can not have any other solution other than $1, b, b^2, \dots, b^{m-1}$. Hence any integer a having order $m \pmod{p}$ must be a power of b . If $c = b^r$, c has order $m \pmod{p} \Leftrightarrow (r, m) = 1$. Thus only $\phi(m)$ integers among $1, b, b^2, \dots, b^{m-1}$ have order $m \pmod{p}$.

That is the number of integer having order $m \pmod{p}$ is $\phi(m)$, if there exists an integer having order $m \pmod{p}$.

Let A_s = number of integer k , $1 \leq k \leq p-1$ which have order $s \pmod{p}$ and if there is no integer having order $s \pmod{p}$ then

$A_s = (0)$. Since each integer k , $1 \leq k \leq p-1$ has some order $m \pmod{p}$ then $m \mid p-1$.

Hence

$$p-1 = \sum_{s \mid p-1} A_s$$

$$p-1 = \sum_{s \mid p-1} \phi(s)$$

Hence

$$(6) \sum_{s|p-1} A_s = \sum_{s|p-1} \varphi(s) = p-1.$$

If $A_s > 0$ then $A_s = \varphi(s)$ otherwise $A_s \leq \varphi(s)$. From (6) we get $A_s = \varphi(s)$ for all s .

$\varphi(p-1) = A_{p-1}$ ie $A_{p-1} = \varphi(p-1)$ implies there exists at least one primitive root (mod p) for each prime $p \geq 3$.

Example 1 : Take $p = 17$.

$p-1 = 16$ Divisors of 16 are 1, 2, 2^2 , 2^3 , 2^4 , .

Integer having order 1 (mod 17) is 1 and $\varphi(1) = A_1$,

order 2 (mod 17) is 16 since $2^{16} \equiv 1 \pmod{17}$ and $\varphi(2) = A_2$.

Order 4 (mod 17) is (4, 13) and $\varphi(4) = 2 = A_4$; order 8 (mod 17) is (2, 8, 9, 12) and $\varphi(8) = 4 = A_8$; and order 16 (mod 17) is { 3, 5, 6, 7, 10, 11, 14, 13}

and $\varphi(16) = 8 = A_{16}$.

Thus $p = 17$ has 8 primitive roots belonging to it.

6.4. THE EXISTENCE OF PRIMITIVE ROOTS MOD p^k .

Consider the case $m = p^k$, where p is an odd prime and $k \geq 2$. To find primitive roots mod p^k . Let a be such a primitive root mod p . To see whether a is primitive root mod p^2 . Now $a^{p-1} \equiv 1 \pmod{p}$, and since $\varphi(p^2) = p(p-1) > p-1$, a is not a primitive root mod p^2 if $a^{p-1} \equiv 1 \pmod{p^2}$. Therefore

$$(7) a^{p-1} \not\equiv 1 \pmod{p^2}$$

is a necessary conditions for a primitive root a mod p to be a primitive root mod p^2 condition (7) is also sufficient for a to be primitive root mod p^2 , and also mod p^k for $k \geq 2$ we have the following theorem.

THEOREM 10 : Let p be an odd prime. Then (i) if a is a primitive root mod p then a is also a primitive root mod p^k for all $k \geq 1$ if and only if (7) holds.

(ii) There exists at least one primitive root a mod p which satisfies (7), hence there exists at least one primitive root mod p^k , if $k \geq 2$.

PROOF : Proof of (ii) Let a be a primitive root mod p . If $a^{p-1} \not\equiv 1 \pmod{p^2}$ there is nothing to prove. On the other hand if $a^{p-1} \equiv 1 \pmod{p^2}$ then $a_1 = a + p$ is another primitive root modulo p , satisfying $a_1^{p-1} \not\equiv 1 \pmod{p^2}$ because

$$a_1^{p-1} = (a+p)^{p-1} = a^{p-1} + (p-1) a^{p-2} p + sp^2$$

$$= a^{p-1} + (p^2 - p) a^{p-2} \pmod{p^2}$$

$$\equiv 1 - p a^{p-2} \pmod{p^2}.$$

Since the second term can not be divisible by p^2 because

if
$$p a^{p-1} \equiv 0 \pmod{p^2}$$

then we have $a^{p-2} \equiv 0 \pmod{p^2}$ contradicting the fact that a is a primitive root mod p .

Hence
$$a_1^{p-1} \not\equiv 1 \pmod{p^2}.$$

Next to prove (i), let a be a primitive root modulo p . If this a is a primitive root mod p^k for all $k \geq 1$, then it is primitive root mod p^2 which implies (7) is true.

Converse part : suppose that a is a primitive root mod p which satisfies (7). To show that a is a primitive root mod p^k for all $k \geq 2$. Let r be the order of a mod p^k . Then to show that $r = \phi(p^k)$. Since $a^r \equiv 1 \pmod{p^k}$,

we have
$$a^r \equiv 1 \pmod{p} \text{ so } \phi(p) \mid r. \text{ We write}$$

(8)
$$r = q \phi(p).$$

Now $r \mid \phi(p^k)$ so $q \phi(p) \mid \phi(p^k)$

But
$$\phi(p^k) = p^{k-1} (p-1).$$

Hence
$$q (p-1) \mid p^{k-1} (p-1)$$

which means $q \mid p^{k-1}$ Therefore $q = p^s$

where $s \leq k-1$; and (8) becomes $r = p^s (p-1)$.

If we prove that $s = k-1$ then $r = \phi(p^k)$ and the proof is complete. Suppose it is not then $s \leq k-2$ and we have $r = p^s (p-1) \mid p^{k-2} (p-1)$ i.e. $\phi(p^{k-1}) = m r$.

Thus, since $\phi(p^{k-1})$ is a multiple of r , this implies

$$a^{\phi(p^{k-1})} \equiv 1, a^{mr} \equiv (a^r)^m \equiv 1 \pmod{p^k} \text{ since } a^r \equiv 1 \pmod{p^k} \text{ which is a contradiction follows from the following theorem.}$$

THEOREM 11 : Let a be a primitive root modulo p such that

(9)
$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then for every $k \geq 2$ we have

(10)
$$a^{\phi(p^{k-1})} \not\equiv 1 \pmod{p^k}.$$

PROOF : The proof is by induction on k . For $k = 2$, (10) reduces to (9). Suppose (10) holds then

$$a^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}} \text{ (Euler-Fermat's Theorem)}$$

so $a^{\varphi(p^{k-1})} = 1 + mp^{k-1}$

where $p \nmid m$. Raising both sides to p^{th} power we get

$$\begin{aligned} a^{\varphi(p^k)} &= (1 + mp^{k-1})^p \\ &= 1 + mp^k + m^2 p(p-1)/2 p^{2(k-1)} + tp^{3(k-1)} \end{aligned}$$

now $2k-1 \geq k+1$ and $3k-3 \geq k+1$ since $k \geq 2$.

Hence we get

$$a^{\varphi(p^k)} \equiv 1 + mp^k \pmod{p^{k+1}}$$

where $p \nmid m$. Hence

$$a^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}.$$

So (10) holds for $k+1$ if it holds for k . This completes the proof of the theorem.

6.5. THE EXISTENCE OF PRIMITIVE ROOTS MODULO $2p^k$

THEOREM 12 : If p is an odd prime and $k \geq 1$ there exists odd primitive roots a modulo p^k . Each such a is also a primitive root mod $2p^k$.

PROOF : If a is a primitive root mod p^k so is $a + p^k$ as shown earlier. One of a or $a + p^k$ is odd. Hence odd primitive roots modulo p^k always exist. Let a be an odd primitive root mod p^k and let r be order of a mod $2p^k$. To show that $r = \varphi(2p^k)$.

Now r divides $\varphi(2p^k)$, and $\varphi(2p^k) = \varphi(2) \varphi(p^k) \varphi(p^k)$.

So r also divides $\varphi(p^k)$. Again $a^r \equiv 1 \pmod{2p^k}$.

so $a^r \equiv 1 \pmod{p^k}$. Hence $\varphi(p^k) \mid r$ since a is primitive root modulo p^k . Therefore $r = \varphi(p^k) = \varphi(2p^k)$, so a is a primitive root mod $2p^k$.

THEOREM 13 : Given $m \geq 1$ where m is not of the form $m = 1, 2, p^k$ or $2p^k$ where p is an odd prime. then for any a with $(a, m) = 1$ we have

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}.$$

So there are no primitive root mod m .

PROOF : we have shown earlier that there are no primitive roots mod 2^k if $k \geq 3$.

Since $m \geq 1$, m has following factorization :

$$m = 2^k p_1^{k_1} \dots p_s^{k_s}.$$

where p_i are odd primes, $s \geq 1$, and $k \geq 0$. Since m is not of the form $1, 2, p^k$ or $2p^k$ we have $k \geq 2$ if $s = 1$ and $s \geq 2$ if $k = 0$ or 1 .

Now

$$\phi(m) = \phi(2^k) \phi(p_1^{k_1}) \dots \phi(p_s^{k_s}).$$

Let $(a, m) = 1$ To prove that $a^{\phi(m)/2} \equiv 1 \pmod{m}$ Let b be a primitive root mod $p_1^{k_1}$ and choose r such that

$$a \equiv b^r \pmod{p_1^{k_1}}.$$

Then we have

$$(11) a^{\phi(m)/2} \equiv b^{r\phi(m)/2} \equiv b^{t\phi(p_1^{k_1})} \pmod{p_1^{k_1}}$$

where

$$t = r \phi(2^k) \phi(p_2^{k_2}) \dots \phi(p_s^{k_s})/2.$$

If $k \geq 2$ the factor $\phi(2^k)$ is even and hence t is an integer. If $k = 0$ or 1 then $s \geq 2$ and the factor $\phi(p_2^{k_2})$ is even so t is an integer in this case. Hence (11) gives us

$$a^{\phi(m)/2} \equiv 1 \pmod{p_1^{k_1}}.$$

Similarly we get

$$(12) a^{\phi(m)/2} \equiv 1 \pmod{p_i^{k_i}}$$

for each $i = 1, 2, \dots, s$. To show that (12) holds mod 2^k . If $k \geq 3$ the condition

$(a, m) = 1$ requires a to be odd and we get by previous theorem

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}.$$

Since $\phi(2^k) | \phi(m)$ this gives

$$(13) a^{\phi(m)/2} \equiv 1 \pmod{2^k}.$$

for $k \geq 3$.

If $k \leq 2$ we have

$$(14) a^{\phi(2^k)} \equiv 1 \pmod{2^k}.$$

But $s \geq 1$ so $\phi(m) = \phi(2^k) \phi(p_1^{k_1}) \dots \phi(p_s^{k_s}) = 2l \phi(2^k)$, where l is an integer. Hence $\phi(2^k) | \phi(m)/2$ and (14) implies (13) for $k \leq 2$. Hence (13) holds for all k . Multiplying (13) and (12) we get $a^{\phi(m)/2} \equiv 1 \pmod{m}$ which proves that a can not be a primitive root mod m .

Example 1 : Let $p = 5$ Find a primitive root mod 5^2 .

Solution : We know 2 is a primitive root mod 5. Since $2 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$

$$2^3 \equiv 3 \pmod{5}, 2^4 \equiv 1 \pmod{5}.$$

Again $2^4 \equiv 1 \pmod{5^2}$ and $2^{20} \equiv 1 \pmod{5^2}$ 2 is a primitive root $\pmod{5^2}$.

Exercise 1 : Show that 3 is a primitive roots $\pmod{5^2}$.

Exercise 2 : Determine all primitive roots of $3^2, 3^3, 3^4, 3^5$.

6.6. INDICES.

DEFINITION : Let a be a primitive root \pmod{m} . For any integer b coprime to m if $b \equiv a^k \pmod{m}$, then k is called as the index of b modulo m relative to a . We write.

$$\text{Ind}_a b = k \text{ if } b \equiv a^k \pmod{m} \text{ or } \text{Ind } b = k.$$

Indices are like logarithms and their properties are also like logarithmic properties.

Example 2 : 2 is a primitive root $\pmod{5}$ and $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1 \pmod{5}$.

It follows that

$$\text{ind}_2 1 = 4, \text{ind}_2 2 = 1, \text{ind}_2 3 = 3, \text{ind}_2 4 = 2.$$

We observe that indices of integers which are congruent modulo n are equal.

If $a \equiv b \pmod{n}$, where $(a, n) = (b, n) = 1$,
 since $r^{\text{inda}} \equiv a \pmod{n}$ and $r^{\text{ind } b} \equiv b \pmod{n}$
 we have $r^{\text{ind } a} \equiv r^{\text{ind } b} \pmod{n}$

THEOREM 14 : Let r be a primitive root of n . If $(a, n) = (b, n) = 1$ we have

$$(a) \text{ind}(ab) = \text{ind } a + \text{ind } b \pmod{\phi(n)}$$

$$(b) \text{ind } a^n = n \text{ind } a \pmod{\phi(n)} \text{ if } n \geq 1$$

$$(c) \text{ind } 1 = 0 \text{ and } \text{ind } r = 1. \text{ if } n > 2.$$

PROOF : By definition of index,

$$r^{\text{ind } a} \equiv a \pmod{n}$$

and $r^{\text{ind } b} \equiv b \pmod{n}$. Multiplying these congruences together we get

$$r^{\text{ind } a + \text{ind } b} \equiv ab \pmod{n}$$

But $r^{\text{ind}(ab)} \equiv ab \pmod{n}$, so that

$$r^{\text{ind } a + \text{ind } b} \equiv r^{\text{ind}(ab)} \pmod{n}.$$

It may happen that $\text{ind } a + \text{ind } b$ exceeds $\phi(n)$.

This gives no problem for by theorem the last equation holds if and only if the order are congruent modulo $\phi(n)$; i.e.

$$\text{ind } a + \text{ind } b \equiv \text{ind } (a b) \pmod{\phi(n)}.$$

To prove (b).

$$\begin{aligned} r^{\text{ind } a^k} &\equiv a^k \pmod{n} \\ \text{while } r^{k \text{ ind } a} &\equiv (r^{\text{ind } a})^k \equiv a^k \pmod{n}, \text{ hence} \end{aligned}$$

$$r^{\text{ind } a^k} \equiv r^{k \text{ ind } a} \pmod{n}$$

As in case (a) we have $\text{ind } a^k \equiv k \text{ ind } a \pmod{\phi(n)}$.

The proof of (c), follow as:

$$r^0 \equiv 1 \pmod{n}, \text{ we have } \text{ind } (1) = 0$$

$$a^1 \equiv a \pmod{n} \Rightarrow \text{ind}_a(a) = 1.$$

6.7. APPLICATION OF INDICES IN SOLVING CONGRUENCE.

The theory of indices can be used to solve certain types of congruence.

For example consider the binomial congruence

$$x^k \equiv a \pmod{n}$$

where n is a positive integer having a primitive root and $\gcd(a, n) = 1$ By theorem 14 this congruence is equivalent to the linear congruence

$$k \text{ ind } x \equiv \text{ind } a \pmod{\phi(n)}.$$

If $d = \gcd(k, \phi(n))$ and $d \nmid \text{ind } a$, there is no solution. But if $d \mid \text{ind } a$, then there are exactly d values of $\text{ind } x$ which will satisfy this last congruence, hence d incongruent solutions of $x^k \equiv a \pmod{n}$.

Consider the case $k = 2$ and $n = p$. We get the quadratic congruence

$$x^2 \equiv a \pmod{p}.$$

This congruence has a solution, if and only if $2 \mid \text{ind } a$; when this condition is fulfilled, there are exactly two solutions. If r is a primitive root of p , then r^k ($1 \leq k \leq p-1$) runs through integers $1, 2, \dots, p-1$, in some order. The even powers of r produces the values of a for which the congruence $x^2 \equiv a \pmod{p}$ is solvable. There are precisely $(p-1)/2$ such choices for a .

Example 1 : Solve the linear congruence $7x \equiv 2 \pmod{9}$.

Solution : We know 2 is a primitive root modulo 9.

$$\begin{array}{ll} \text{Also } 2^1 \equiv 2 \pmod{9} & 2^4 \equiv 7 \pmod{9} \\ 2^2 \equiv 4 \pmod{9} & 2^5 \equiv 5 \pmod{9} \\ 2^3 \equiv 8 \pmod{9} & 2^6 \equiv 1 \pmod{9}. \end{array}$$

Index of 7 is 4 and 2 is 1.

Now $7x \equiv 2 \pmod{9}$ is equivalent to

$\text{Ind } 7 + \text{Ind } x \equiv \text{Ind } 2 \pmod{\phi(9)}$

$$\equiv \text{Ind } 2 \pmod{6}$$

or $4 + \text{Ind } x \equiv 1 \pmod{6}$

or $\text{Ind } x \equiv -3 \pmod{6}$.

Hence $x \equiv 2^3 \pmod{9}$ (Since $-3 \equiv 3 \pmod{6}$)

or $x \equiv 8 \pmod{9}$.

Thus solutions of $7x \equiv 2 \pmod{9}$ are of the form $9t + 8$ for $t = 0, \pm 1, \pm 2, \dots$

Example 2 : Solve the congruence

$$11x^3 \equiv 2 \pmod{23}.$$

Solution : Here $p = 23$, 5 is a primitive root of 23. Also

$$5^1 \equiv 5 \pmod{23}$$

$$5^6 \equiv 8 \pmod{23}$$

$$5^2 \equiv 2 \pmod{23}$$

$$5^7 \equiv 17 \pmod{23}$$

$$5^3 \equiv 10 \pmod{23}$$

$$5^8 \equiv 16 \pmod{23}$$

$$5^4 \equiv 4 \pmod{23}$$

$$5^9 \equiv 11 \pmod{23}$$

$$5^5 \equiv 20 \pmod{23}$$

$$5^{10} \equiv 9 \pmod{23}$$

$11x^3 \equiv 2 \pmod{23}$ is equivalent to

$$\text{Ind } 11 + 3 \text{Ind } x \equiv \text{Ind } 2 \pmod{22}$$

$$\text{Or } 9 + 3 \text{Ind } x \equiv \text{Ind } 2 \pmod{22}$$

$$\text{or } 3 \text{Ind } x \equiv -7 \pmod{22}$$

$$\text{or } 3 \text{Ind } x \equiv 15 \pmod{22}$$

$$\text{or } \text{Ind } x \equiv 5 \pmod{23}$$

$$\text{Hence } x \equiv 5^5 \pmod{23}$$

$$\text{or } x \equiv 20 \pmod{23}.$$

Thus $x = 23t + 20$, $t = 0, \pm 1, \pm 2, \dots$ are all solutions of the given congruence.

Exercise : Solve the congruence

$$4x^9 \equiv 7 \pmod{13}.$$

THEOREM 15 : Let n be an integer having a primitive root and let $\gcd(a, n) = 1$, then the congruence $x^k \equiv a \pmod{n}$ has solution if and only if

$$(15) \quad a^{\varphi(n)/d} \equiv 1 \pmod{n},$$

where $d = \gcd(k, \varphi(n))$; if it has a solution there are exactly d solutions modulo n .

PROOF : $a^{\varphi(n)/d} \equiv 1 \pmod{n}$, implies $\varphi(n)/d \text{ Ind } a = \text{Ind } 1 \pmod{n} \equiv 0 \pmod{n}$ which holds if and only if $d \mid \text{ind } a$, which is a necessary and sufficient conditions for the congruence $x^k \equiv a \pmod{n}$ to be solvable.

Corollary : Let p be a prime and $\gcd(a, p) = 1$. Then the congruence $x^k \equiv a \pmod{p}$ has a solution if, and only if $a^{p-1/d} \equiv 1 \pmod{p}$, where $d = \gcd(k, p-1)$.

Example 3 : Solve the congruence

$$x^3 \equiv 4 \pmod{13}.$$

Here, $d = \gcd(3, \varphi(13)) = \gcd(3, 12) = 3$.

So $\varphi(13)/d = 4$. Since $4^4 \equiv 9 \not\equiv 1 \pmod{13}$, the congruence is not solvable.

6.8. THE DISCRETE LOGARITHM

DEFINITION: Suppose r is a primitive root modulo n . If $r^x \equiv y \pmod{n}$ then the discrete logarithm or index of y (to the base r) is

$$\text{ind}_r(y) = x \pmod{\varphi(n)}.$$

Example 1 : 3 is a primitive root of 17. We have $3^8 \equiv -1 \pmod{17}$ and $3^{12} \equiv 4 \pmod{17}$.

So $\text{ind}_3(-1) = 8$ and $\text{ind}_3(4) = 12$.

Example 2 : We use the properties of discrete logarithm to solve the congruence

$$7^x \equiv 4 \pmod{17}.$$

Solution : 3 is a primitive root mod 17.

Taking the index to the base 3 we get

$$\text{ind}_3(7^x) \equiv \text{ind}_3(4)$$

$$\text{or } x \text{ ind}_3(7) \equiv \text{ind}_3(4) \pmod{\varphi(17)}.$$

$$\text{Since } \text{ind}_3(7) = 11 \text{ and } \text{ind}_3(4) = 12$$

solving the equation is equivalent to

$$11x \equiv 12 \pmod{16}.$$

The solution is $x \equiv 4 \pmod{16}$.

EXERCISES

1. Find the index of 5 relative to each of the primitive roots of 13.
2. Using theory of indices find the remainder where $3^{24} \cdot 5^{13}$ is divided by 17.
3. If r is a primitive root of n , verify that, $\text{ind}_r(-1) = \text{ind}_r(\varphi(n)) = \varphi(n)/2$.
4. Solve the congruence $x^3 \equiv 5 \pmod{13}$.
5. Solve the congruences
 - (i) $7x^3 \equiv 3 \pmod{11}$.
 - (ii) $4x \equiv 19 \pmod{23}$
 - (iii) $57^x \equiv 2 \pmod{13}$.
6. Determine whether the congruence $x^5 \equiv 13 \pmod{23}$ is solvable.
7. For which values of b the congruence $9^x \equiv b \pmod{13}$ is solvable..
8. Using a table of indices for a primitive root of 11, solve the congruence
 - (i) $7x^3 \equiv 3 \pmod{11}$.
 - (ii) $3x^4 \equiv 5 \pmod{11}$
 - (iii) $x^8 \equiv 10 \pmod{11}$.
9. If r and r' are both primitive roots of n , show that for $\gcd(a, n) = 1$

$$\text{ind}_r a \equiv (\text{ind}_r a)(\text{ind}_{r'} r) \pmod{\varphi(n)}.$$
10. Let p be an odd prime. Find all solutions of $x^{p-1} \equiv 2 \pmod{p}$.
11. Let a be a primitive root modulo prime p . Then prove that
 - (i) $a^{(p-1)/2} \equiv -1 \pmod{p}$.
 - (ii) If a' is another primitive root modulo p , then aa' is not a primitive root modulo p .
12. Let p be an odd prime. Prove that a has order 2 mod p if and only if $a \equiv -1 \pmod{p}$.
13. Prove that n is a prime if and only if $\text{ord}_n(a) = n - 1$ for some a .
14. If $(a, n) = (b, n) = 1$ and if $(\text{ord}_n(a), \text{ord}_n(b)) = 1$, prove that $\text{ord}_n(ab) = \text{ord}_n(a)\text{ord}_n(b)$.
15. Show that 18 is a primitive root modulo 37. Is it also a primitive root modulo 37^2 ?



QUADRATIC RESIDUES AND QUADRATIC RECIPROCITY LAWS

7.1. QUADRATIC RESIDUES

In chapter 3, the problem of solving polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

are dealt with. Here we will consider quadratic congruence of the form

$$(1) \quad x^2 \equiv a \pmod{p}$$

where p is an odd prime and $(a, p) = 1$.

Lagrange's theorem tells that a polynomial congruence

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \equiv 0 \pmod{p},$$

$(a_n, p) = 1$ has at most n solutions.

So the quadratic congruence (1) has at most two solutions. If x is a solution so is $-x$, hence (1) has either no solution or 2 solutions.

Now consider the general quadratic congruence

$$(2) \quad ax^2 + bx + c \equiv 0 \pmod{p}$$

where p is an odd prime and $(a, p) = 1$. p is an odd prime implies that $(4a, p) = 1$. Then (2) is equivalent to

$$(3) \quad 4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

$$\text{But } 4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac).$$

So (3) may be expressed as

$$(4) \quad (2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}.$$

Now put $y = 2ax + b$ and $d = b^2 - 4ac$ to get

$$(5) \quad y^2 \equiv d \pmod{p}.$$

If $x \equiv x_0 \pmod{p}$ is a solution of (2) then

$$y \equiv 2ax_0 + b \pmod{p}$$

satisfies the congruence (5). Conversely if $y \equiv y_0 \pmod{p}$ is a solution of (5), then

$$2ax \equiv y_0 - b \pmod{p}$$

can be solved to obtain solution of (2).

Thus, the problem of finding a solution to the quadratic congruence (2) is equivalent to that of finding a solution to linear congruence and a quadratic congruence of the form (1).

It is clear that if $x = x_0$ is a solution of (1) and $x = p - x_0$ is another solution.

Example 1 : Solve $x^2 \equiv 5 \pmod{29}$.

Solution :

$$x^2 \equiv 5 \equiv 5 + 29 \equiv 34 \equiv 63 \equiv 92 \equiv 121 \equiv 11^2 \pmod{p} \text{ (i.e. add multiple of } p \text{ till we get a square number).}$$

Hence the required solutions are

$$x \equiv 11, 29 - 11 \pmod{29}$$

$$\equiv 11, 18 \pmod{29}.$$

Example 2 : Solve $x^2 \equiv 4 \pmod{13}$.

Solution :

$$x^2 \equiv 4 \equiv 17 \equiv 30 \equiv 43 \equiv 56 \equiv 69 \equiv 82 \equiv 95 \equiv 108 \equiv 121 \equiv 11^2 \pmod{13}$$

So solution are $x \equiv 11, 13 - 11 \pmod{29}$

$$\equiv 11, 2 \pmod{29}.$$

Example 3 : Solve the congruence

$$2x^2 - 5x + 3 \equiv 0 \pmod{29}.$$

Solution : The congruence is reduced to $y^2 \equiv d \pmod{29}$

where

$$d = b^2 - 4ac = 25 - 24 = 1$$

and to solve the congruence $y^2 \equiv 1 \pmod{29}$

with solution $y \equiv 1, 28 \pmod{29}$.

Next solve the linear congruence

$$4x \equiv 1 - (-5) \equiv 6 \pmod{29}$$

$$4x \equiv 28 - (-5) = 33 \equiv 4 \pmod{29}$$

$$x \equiv 6 \cdot 4^{28-1} \pmod{29} \equiv 6 \cdot 4^{27} \pmod{29}.$$

To calculate $4^{27} \pmod{29}$.

$$4^{28} \equiv 1 \pmod{29}.$$

\Rightarrow

$$4^{27} \equiv 4^{-1} \pmod{29}.$$

To calculate $4^{-1} \pmod{29}$.

$$4 \cdot 4^{-1} \equiv 1 \pmod{29}$$

$$\Rightarrow 4^{-1} = 22.$$

$$\text{Hence } x \equiv 6 \cdot 22 \pmod{29} \equiv 16 \pmod{29}$$

$\Rightarrow x \equiv 16 \pmod{29}$ is a solution which satisfies the original quadratic congruence also.

$$\text{Next } 4x \equiv 4 \pmod{29}$$

$$\Rightarrow x \equiv 1 \pmod{29}.$$

So $x \equiv 1 \pmod{29}$ is a solutions of the congruence $4x \equiv 4 \pmod{29}$ hence of the original quadratic congruence.

Hence the two solution are $x \equiv 1, 16 \pmod{29}$.

Exercise 1 : Solve $5x^2 - 6x + 2 \equiv 0 \pmod{13}$.

Exercise 2 : Solve $x^2 \equiv 52 \pmod{101}$.

DEFINITION : If the congruence $x^2 \equiv a \pmod{p}$, where p is a prime and $(a, p) = 1$ has a solution then a is said to be a quadratic residue modulo p . We write $a \text{Rp}$ Otherwise a is called quadratic nonresidue modulo p . We write $a \text{Np}$.

If $a \equiv b \pmod{p}$ then $(a, p) = (b, p)$ so a is a quadratic residue modulo p if and only if b is a quadratic residue modulo p .

Example : Consider $p = 17$. Find all quadratic residues and non residues of 17.

Solution : We find a among $[1, 2, 3, \dots, 16]$ modulo 17 which satisfy the congruence

$$x^2 \equiv a \pmod{17}.$$

The squares of the integer 1, 2, 3, ..., 16 are

$$1^2 \equiv 16^2 \equiv 1$$

$$2^2 \equiv 15^2 \equiv 4$$

$$3^2 \equiv 14^2 \equiv 9$$

$$4^2 \equiv 13^2 \equiv 16$$

$$5^2 \equiv 12^2 \equiv 8$$

$$6^2 \equiv 11^2 \equiv 2$$

$$7^2 \equiv 10^2 \equiv 15$$

$$8^2 \equiv 9^2 \equiv 13.$$

So the quadratic residues of 17 are 1, 2, 4, 8, 13, 15, 16 while non residues are 3, 5, 6, 7, 10, 11, 12, 14.

Remark : The number of quadratic residue of p are same as the number of quadratic non residues.

Example : If $p = 19$ then $(p-1)/2 = (19-1)/2 = 9$.

Hence $x^2 \equiv 1 \pmod{19}$ has exactly 9 solutions, namely

$$\begin{aligned} x &\equiv 1^2, 2^2, \dots, 9^2 \pmod{19} \\ &\equiv 1, 4, 9, 16, 6, 17, 11, 7, 5 \pmod{19}. \end{aligned}$$

THEOREM 1 : If $(a, p) = 1$ then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

PROOF : By Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$.

This $\Rightarrow (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$
 \Rightarrow either $a^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ i.e. $a^{(p-1)/2} \equiv 1 \pmod{p}$

or $a^{(p-1)/2} + 1 \equiv 0 \pmod{p}$ i.e. $a^{(p-1)/2} \equiv -1 \pmod{p}$.

But not both since in that case $(a^{(p-1)/2} + 1) - (a^{(p-1)/2} - 1) = 2$ would be divisible by p which is impossible.

Hence the theorem is proved.

THEOREM 2 : The congruence

$$(6) \ x^{(p-1)/2} \equiv 1 \pmod{p}$$

has exactly $p-1/2$ solutions congruent modulo p and $p-1/2$ solutions incongruent modulo p . The congruent solutions are

$$x \equiv 1^2, 2^2, \dots, (p-1/2)^2 \pmod{p}.$$

PROOF : Let $S = \{ 1^2, 2^2, \dots, (p-1/2)^2 \}$.

If t^2 is an integer of S , then $(t, p) = 1$.

So by Fermat's theorem we have

$$t^{p-1} \equiv 1 \pmod{p}$$

which $\Rightarrow (t^2)^{p-1/2} \equiv 1 \pmod{p}$.

Thus every integer of S is a solution.

All the integers of S are all incongruent \pmod{p} .

For if $u^2 \equiv v^2 \pmod{p}$ such that $1 \leq u \leq v \leq (p-1)/2$ then it would follow that $(u - v)(u + v)$ would be divisible by p . But this is impossible since both $u - v$ and $u + v$ are numerically less than p . Moreover $(p-1)/2$ divides $p-1$. Therefore (6) has exactly $(p-1)/2$ solutions.

Since there are $p-1/2$ solutions of the congruence $x^2 \equiv a \pmod{p}$, there are exactly $p-1/2$ incongruent solutions mod p . Hence we have the following .

THEOREM 3 : Let p be an odd prime. Then every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic non-residues mod p . The quadratic residues belong to the residue classes containing the numbers.

$$(7) \quad 1^2, 2^2, 3^2, \dots ((p-1)/2)^2.$$

7.2. LEGENDRE'S SYMBOL AND ITS PROPERTIES.

DEFINITION : Let p be a prime. We define Legendre's symbol (a/p) as follows:

$$(8) \quad \left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \in R_p \\ -1 & \text{if } a \in N_p. \end{cases}$$

$$(a/p) = 0 \text{ if } p|a.$$

Example : $(1/p) = 1$, p is a prime.

$$(a^2/p) = 1 \quad (8/17) = 1 \quad (7/19) = 1.$$

$(7/11) = 1$, since 7 is a quadratic residue modulo 11.

THEOREM 4 : (Euler's criterion). The congruence

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1$$

has a solution if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

PROOF : Let

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Then a is solution of

$$x^{(p-1)/2} \equiv 1 \pmod{p}.$$

Therefore a is congruent mod p to one of the integers $1^2, 2^2, \dots ((p-1)/2)^2$. Let this integer be t^2 . That is $t^2 \equiv a \pmod{p}$. Therefore $x = t$ is a solution of $x^2 \equiv a \pmod{p}$.

Converse part : Let the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution say

$$x \equiv b \pmod{p}. \text{ It follows that } b^2 \equiv a \pmod{p}.$$

Hence $a^{p-1/2} \equiv (b^2)^{p-1/2} \equiv b^{p-1} \pmod{p} \equiv 1 \pmod{p}$ by Fermat's theorem.

Example : Show that $x^2 \equiv 18 \pmod{79}$ is soluble.

Solution : Here $p = 79$, $(p-1)/2 = 39$, $a = 18$, $a^{(p-1)/2} \equiv 18^{39} \equiv 1 \pmod{79}$.

Hence the given congruence is solvable. The solution can be found as in previous example. They are $x \equiv 27, 52 \pmod{79}$.

THEOREM 5 : $x^2 \equiv a \pmod{p}$, $(a, p) = 1$ has no solution if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.

PROOF : Suppose $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Then it follows $a^{(p-1)/2} \not\equiv 1 \pmod{p}$.

Therefore $x^2 \equiv a \pmod{p}$ has no solution.

Conversely suppose $x^2 \equiv a \pmod{p}$ be not solvable.

Then it follows that $a^{(p-1)/2} \equiv 1 \pmod{p}$.

So $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Example 1. $x^2 \equiv 10 \pmod{19}$ has no solution since $10^{(19-1)/2} \equiv 10^9 \equiv -1 \pmod{19}$.

Example 2. $x^2 \equiv 10 \pmod{11}$ has no solution since $10^{(11-1)/2} = 10^5 \equiv -1 \pmod{11}$.

THEOREM 6 : (Euler's criterion) $x^2 \equiv a \pmod{p}$, $(a, p) = 1$ is solvable if and only if

$a^{(p-1)/2} \equiv 1 \pmod{p}$ and has no solution if and only if

$a^{(p-1)/2} \equiv -1 \pmod{p}$.

Corollary : (Fermat's theorem). From the above theorem we deduce Fermat's theorem. Because there are two possibilities. The congruence $x^2 \equiv a \pmod{p}$ has a solution or has no solution.

We have either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \text{ or}$$

$$a^{(p-1)/2} \equiv (-1) \pmod{p}.$$

Squaring both the sides we obtain

$$a^{p-1} \equiv 1 \pmod{p}.$$

Since $(a/p) = +1$ if $a \in R_p$

$= -1$ if $a \in N_p$

in Euler's Criterion we replace the right hand side by (a/p) and we have,

RESULT : Let p be an odd prime then for all a we have

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}.$$

SOME PROPERTIES OF LEGENDRE'S SYMBOL

THEOREM 7 : Legendre's symbol (a/p) is a completely multiplicative function.

PROOF : To prove that $(ab/p) = (a/p) (b/p)$ for all a and b .

(i) If $p|a$ or $p|b$ then $p|ab$. Now $p|a \Rightarrow (a/p) = 0$ or $p|b \Rightarrow (b/p) = 0$.
and $p|ab \Rightarrow (ab/p) = 0$

Hence $(ab/p) = (a/p) (b/p)$.

(ii) If $p \nmid a$ and $p \nmid b$ then $p \nmid ab$ and we have

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p) (b/p) \pmod{p}$$

by theorem 6 But each of (ab/p) , (a/p) and (b/p) is 1 or -1 so the difference $(ab/p) - (a/p)(b/p)$ is either 0, 2 or -2 .

THEOREM 8 : If $a \equiv b \pmod{p}$. Then $(a/p) = (b/p)$.

PROOF : If a is a quadratic residue modulo p so is b and if a quadratic non residue modulo p then so is b .

THEOREM 9 : $(a_1/p) (a_2/p) \dots (a_k/p) = (a_1 a_2 \dots a_k/p)$.

$$\begin{aligned} \text{PROOF : } (a_1/p) (a_2/p) \dots (a_k/p) &\equiv a_1^{p-1/2} \dots a_k^{p-1/2} \pmod{p} \\ &\equiv (a_1 \dots a_k)^{p-1/2} \pmod{p} \\ &\equiv (a_1 \dots a_k/p) \pmod{p} \end{aligned}$$

Since $(a_1/p), (a_2/p) \dots (a_k/p)$ are all equal to $+1$ or -1 .

Similarly $(a_1 \dots a_k/p) = +1$ or -1 .

Hence $(a_1/p) (a_2/p) \dots (a_k/p) = (a_1 a_2 \dots a_k/p)$.

THEOREM 10 : If $(a/p) = 1$, then $(a^2/p) = 1$

PROOF : The theorem is trivial since a^2 is a quadratic residue of every p .

Corollary : $(a b^2/p) = (a/p)$.

PROOF : $(a b^2/p) = (a/p) (b^2/p) = (a/p)$.

THEOREM 11 : For every odd prime p we have

$$(9) \quad (-1/p) = (-1)^{p-1/2} = \begin{cases} 1 & \text{if } p=4k+1 \\ -1 & \text{if } p=4k+3 \end{cases}$$

PROOF : By Euler's Criterion we have $(-1/p) = (-1)^{p-1/2} \pmod{p}$

Since the values of both sides of congruence are 1 or -1 the two members are equal.

That is

$$(-1/p) = (-1)^{p-1/2}$$

$$\text{If } p = 4k + 1, (-1)^{p-1/2} = (-1)^{2k} = +1$$

$$\text{If } p = 4k + 3, (-1)^{p-1/2} = (-1)^{2k+1} = -1$$

Hence proved.

THEOREM 12 : For every odd prime p we have

$$(10) \quad (2/p) = (-1)^{\frac{p^2-1}{8}} \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

PROOF : we know

$$(A) \quad \left\{ \begin{array}{l} (p-1) \equiv 1(-1)^1 \pmod{p} \\ 2 \equiv 2(-1)^2 \pmod{p} \\ p-3 \equiv 3(-1)^3 \pmod{p} \\ 4 \equiv 4(-1)^4 \pmod{p} \\ \vdots \\ r \equiv (p-1)/2 (-1)^{(p-1)/2} \pmod{p}, \end{array} \right.$$

where r is either $p-1/2$ or $p-(p-1/2)$ multiplying together in the set (A) we obtain

$$\Rightarrow \quad 2, 4, 6, \dots, (p-1) \equiv (p-1/2)! (-1)^{1+2+\dots+(p-1)/2} \pmod{p}$$

$$\Rightarrow \quad 2^{(p-1)/2} (p-1/2)! \equiv (p-1/2)! (-1)^{p^2-1/8} \pmod{p}.$$

$$\text{Since } (p, (p-1/2)!) = 1 \text{ canceling } ((p-1)/2)!$$

from both sides we obtain

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod{p}.$$

$$\text{But by Euler's criterion } 2^{(p-1)/2} \equiv (2/p) \pmod{p}.$$

and since each member is $+1$ or -1 the two members are equal completing the proof of the theorem.

7.3. GAUSS' LEMMA

We now give another Criterion due to Gauss which involves a simpler calculation and applicable for large n .

THEOREM 13 : (Gauss' lemma) Assume $(a, p) = 1$ and consider the least positive residues modulo p of the following $(p-1/2)$ multiples of a .

$$(11) \quad a, 2a, 3a, \dots, (p-1/2)a.$$

If n denotes the number of these residues which exceed $p/2$, then

$$(a/p) = (-1)^n.$$

PROOF : Let r_1, r_2, \dots, r_n denote the residues that exceed $p/2$, and let s_1, s_2, \dots, s_k denote the remaining residues. The r_i and s_j are all distinct, and non zero.

Further $n + k = (p-1)/2$. Now $0 < p-r_i < p/2$, $i = 1, 2, \dots, n$, and the numbers $p-r_i$ are distinct. Also no $p-r_i$ is an s_j for if $p-r_i = s_j$ then $r_i \equiv \rho a$, $s_j \equiv \sigma a$, for some ρ, σ , $1 \leq \rho \leq p-1/2$, $1 \leq \sigma \leq (p-1)/2$, and $p - \rho a \equiv \sigma a \pmod{p}$. Since $(a, p) = 1$ this implies $a(\rho + \sigma) \equiv 0$, $(\rho + \sigma) \equiv 0 \pmod{p}$ which is impossible by the nature of ρ and σ . Thus $p-r_1, p-r_2, \dots, p-r_n, s_1, s_2, \dots, s_k$ are all distinct, are all at least 1 and less than $p/2$.

They are just the integer $1, 2, \dots, (p-1)/2$ in some order. Multiplying them together we have

$$\begin{aligned} & (p-r_1)(p-r_2) \dots (p-r_n) s_1 s_2 \dots s_k \\ &= 1 \cdot 2 \cdot 3 \dots p-1/2. \end{aligned}$$

and then

$$\begin{aligned} & (-r_1)(-r_2) \dots (-r_n) s_1 s_2 \dots s_k \equiv 1 \cdot 2 \dots p-1/2 \pmod{p} \\ \Rightarrow & (-1)^n r_1 r_2 \dots r_n s_1 s_2 \dots s_k \equiv 1 \cdot 2 \dots p-1/2 \pmod{p} \\ \Rightarrow & (-1)^n 2a \dots p-1/2 a \equiv 1 \cdot 2 \cdot 3 \dots p-1/2 \pmod{p} \\ \Rightarrow & (-1)^n a^{p-1/2} (p-1)/2! \equiv (p-1)/2! \pmod{p} \end{aligned}$$

Since $((p-1)/2!, p) = 1$, cancelling $(p-1)/2!$ from both sides we have

$$\begin{aligned} & (-1)^n a^{p-1/2} \equiv 1 \pmod{p} \\ \Rightarrow & (-1)^n \equiv a^{p-1/2} \equiv (a/p) \pmod{p} \text{ by Euler's criterion.} \end{aligned}$$

Hence
$$(a/p) = (-1)^n.$$

THEOREM 14 : Let n denotes the number of those residues which exceed $p/2$ then

$$n = \sum_{t=1}^{(p-1)/2} [ta/p] + (a-1)^{(p^2-1)/8} \pmod{2}.$$

In particular, if n is odd we have
$$n \equiv \sum_{t=1}^{(p-1)/2} [ta/p] \pmod{2}.$$

PROOF : Consider the numbers

$$a, 2a, 3a, \dots, (p-1/2)a.$$

Take ta and divide it by p then

$$ta/p = [ta/p] + \{ta/p\}, \text{ where } 0 < \{ta/p\} < 1.$$

So $ta \equiv p [ta/p] + p \{ta/p\} = p [ta/p] + t_i$, for some t_i

where $0 < t_i < p$.

$t_i = ta - p [ta/p]$ is the least positive residue of ta modulo p . Now

$$\{t_1, t_2, \dots, t_{(p-1)/2}\} = \{r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_k\}$$

$$\text{and } \{1, 2, \dots, p-1/2\} = \{r_1, r_2, \dots, r_n, s_1, \dots, s_k\}.$$

So since $(a, p) = 1$, whether a is odd or even, we have

$$\sum_{t=1}^{(p-1)/2} ta \equiv \sum_{t=1}^{p-1/2} p [ta/p] + \sum_{i=1}^{p-1/2} t_i$$

$$\equiv \sum_{t=1}^{p-1/2} p [ta/p] + \sum_{i=1}^n r_i + \sum_{j=1}^k s_j$$

and

$$\sum_{t=1}^{p-1/2} t = \sum_{i=1}^n (p-r_i) + \sum_{j=1}^k s_j$$

$$= np - \sum_{i=1}^n r_i + \sum_{j=1}^k s_j$$

and hence by subtraction,

$$(a-1) \sum_{t=1}^{(p-1)/2} t = p \left(\sum_{t=1}^{p-1/2} [ta/p] - n \right) + 2 \sum_{i=1}^n r_i.$$

But

$$\sum_{t=1}^{(p-1)/2} t = 1 + 2 + \dots + (p-1)/2 = p^2-1/8.$$

So we have

$$(a-1) (p^2-1)/8 \equiv \sum_{t=1}^{(p-1)/2} [ta/p] - n \pmod{2}.$$

If a is odd, this implies

$$n \equiv \sum_{t=1}^{(p-1)/2} [ta/p] \pmod{2}.$$

If

$$a = 2, \text{ it implies } n \equiv p^2-1/8.$$

Since

$$[2t/p] = 0 \text{ for } 0 \leq t \leq p-1/2$$

we get

$$(2/p) = (-1)^{p^2-1/8}$$

which is the theorem 12.

7.4. QUADRATIC RECIPROCITY LAW AND ITS APPLICATION.

THEOREM 15 : If p and q are distinct odd primes, then

$$(12) \quad (p/q) (q/p) = (-1)^{(p-1)(q-1)/4}.$$

PROOF : By Gauss Lemma (theorem 13) and theorem 14 we have

$$(q/p) = (-1)^n$$

where

$$n \equiv \sum_{t=1}^{(p-1)/2} [tq/p] \pmod{2}.$$

Similarly

$$(p/q) = (-1)^m,$$

where

$$m \equiv \sum_{s=1}^{(q-1)/2} [sp/q] \pmod{2}.$$

Hence

$$(p/q) (q/p) = (-1)^{m+n}$$

where

$$m+n = \sum_{t=1}^{(p-1)/2} [tq/p] + \sum_{s=1}^{(q-1)/2} [sp/q].$$

Let s be the set of all pairs of integers (x,y) satisfying

$$1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2.$$

The set has $(p-1)(q-1)/4$ members. Separate the set into two mutually exclusive subsets S_1 and S_2 according as $qx > py$ or $qx < py$. There are no pairs (x,y) in S such that $qx = py$. S_1 is the set of all pairs (x,y) such that

$$1 \leq x \leq (p-1)/2,$$

$$1 \leq y \leq qx/p.$$

The number of pairs in S_1 is seen to be $\sum_{x=1}^{(p-1)/2} [qx/p]$. Similarly the

number of pairs (x, y) in S_2 s.t. $1 \leq y \leq q-1/2$,

$$1 \leq x \leq py/q \text{ is}$$

$$\sum_{y=1}^{(q-1)/2} [py/q]. \text{ Thus we have } m + n = (p-1)/2 (q-1)/2.$$

Hence

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

THEOREM 16 : If $8k + 7$ is a prime then it divides M_{4k+3} .

PROOF : We have proved in theorem 12 that 2 is a quadratic residue of prime of the form $8k-1$, i.e. of the form $8k+7$. Hence by Euler's criterion

$$2^{8k+7-1/2} \equiv 1 \pmod{8k+7}.$$

This implies

$$2^{4k+3} \equiv 1 \pmod{8k+7}$$

$$\Rightarrow 2^{4k+3} - 1 \equiv 0 \pmod{8k+7}$$

$$\text{i.e. } 8k+7 \mid M_{4k+3}$$

This proves the theorem.

Example : Apply the above theorem to find a factor each of some of the Mersenne numbers M_p where p is a prime ≤ 257 .

Solution : Since by the theorem $8k + 7$ divides M_{4k+3}

k	$8k + 7$	$4k + 3$	Factor of M_{4k+3}
2	23	11	Hence $23 \mid M_{11}$
5	47	23	$47 \mid M_{23}$
20	167	83	$167 \mid M_{83}$
32	263	131	$263 \mid M_{131}$
44	359	179	$359 \mid M_{179}$
47	383	191	$383 \mid M_{191}$
59	479	239	$479 \mid M_{239}$
62	503	251	$503 \mid M_{251}$

THEOREM 17 : -2 is a quadratic residue of p if and only if p is of the form $8k+1$, or $8k+3$

PROOF : $(-2/p) = (-1/p) (2/p)$.

$$\begin{aligned} (-2/p) &= (1) (1) = 1 \text{ if } p = 8k + 1 \\ &= (-1) (-1) = 1 \text{ if } p = 8k + 3 \\ &= (1) (-1) = -1 \text{ if } p = 8k + 5 \\ &= (-1) (1) = -1 \text{ if } p = 8k + 7. \end{aligned}$$

The theorem is therefore proved.

THEOREM 18 : 3 is a quadratic residue of p if and only if p is of the form $12k \pm 1$.

PROOF : Every prime $p > 3$ has one of the forms $12k + 1$, $12k - 1$, $12k + 5$ and $12k - 5$. Let $p = 2k + 1$.

Then

$$\left(\frac{3}{p}\right) = \left(\frac{12k+1}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

If $p = 12k - 1 = 4(3k - 1) + 3$ then

$$\left(\frac{3}{p}\right) = \left(\frac{12k+1}{3}\right) = (1) \left(\frac{-1}{3}\right) = 1.$$

If $p = 12k + 5 = 4(3k+1)+1$. Then

$$\left(\frac{3}{p}\right) = \left(\frac{12k+5}{3}\right) = \left(\frac{-1}{3}\right) = 1.$$

If $p = 12k - 5 = 4(3k-2) + 3$. Then

$$\left(\frac{3}{p}\right) = \left(\frac{12k-5}{p}\right) = -\left(\frac{1}{3}\right) = 1.$$

This proves the theorem.

Example : -3 is a quadratic residue of p if and only if p is of the form $6k + 1$ and quadratic non-residue if and only if p is of the form $6k + 5$.

Solution : p is odd, hence

$$(13) \quad p \equiv 1 \pmod{2}$$

$$(-3/p) = (-1/p) (3/p)$$

$$= (p/3) \text{ if } p = 4k + 1$$

$$(-3/p) = (-1/p) (3/p) = (p/3) \text{ if } p = 4k + 3$$

It follows that $(-3/p) = 1$ if and only if p is a quadratic residue of 3. This implies

$$(14) \quad p \equiv 1 \pmod{3}.$$

From (13) and (14) we get $p \equiv 1 \pmod{6}$ i.e.,

$$p = 6k + 1$$

-3 is a quadratic non-residue of a prime if and only if p is the form $6k + 5$ or $6k + 1$.

Example : 5 is a quadratic residue of a prime p if and only if p is of the form $10k \pm 1$.

Solution : Every odd prime p has one of the forms $10k \pm 1$ and $10k \pm 3$. Let $p = 10k \pm 1$.

Then $p = 10k + 1$. Then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{10k+1}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Let $p = 10k - 1$. Then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{10k-1}{5}\right) = \left(\frac{-1}{5}\right) = 1.$$

Let $p = 10k + 3$. Then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{10k+3}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Let $p = 10k - 3$. Then

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{-3}{5}\right) = \left(\frac{2}{5}\right) = \left(\frac{5^2-1}{8}\right) = (-1)^3 = -1.$$

Exercise 1 : Prove that 5 is a quadratic non-residue of a prime p if and only if p is of the form $10k + 3$.

Exercise 2 : Prove that -5 is a quadratic residue p if and only if p is of the form $20k + 1$, $20k + 3$, $20k + 7$ or $20k + 9$.

Exercise 3 : Prove that 7 is a quadratic residue of p if and only if p is of the form $28k \pm 1$, $28k \pm 3$ or $28k \pm 9$.

Exercise 4 : Prove that 10 is a quadratic residue of p if and only if p is of the form $40k \pm 1$, $40k \pm 3$, $40k \pm 9$ or $40k \pm 13$.

Example : Find all quadratic residues of 35.

Solution : $35 = 5 \times 7$ and $(5, 7) = 1$. Therefore the quadratic residues of 35 are those integers, less than 35, which are quadratic residues of both 5 and 7 . The quadratic residues of 5 which are less than 35 are

1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 26, 29, 31, and 34.

The quadratic residues of 7 which are less than 35 are

1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, and 32.

Hence the quadratic residues of 35 are those integers which are common to both the above lists, namely

1, 4, 9, 11, 16 and 29.

Exercise : Find the quadratic residues of 25.

Solution : $25 = 5^2$. Every quadratic residue of 5 is a quadratic residue of 25 and vice versa . Thus the least quadratic residues of 25 are those quadratic residues of 5 which are less than 5. The least quadratic residue of 5 are 1 and 4. Hence quadratic residues of 25 are 1, 4, 6, 9, 11, 14, 16, 19, 21, and 24.

Exercise : Find all quadratic residue of 50.

Example : Evaluate

$$\left(\frac{-42}{61} \right).$$

Solution :

$$\left(\frac{-42}{61} \right) = \left(\frac{-1}{61} \right) \left(\frac{3}{61} \right) \left(\frac{3}{61} \right) \left(\frac{7}{61} \right)$$

$$\left(\frac{-1}{61} \right) = (-1)^{61-1/2} = 1.$$

$$\left(\frac{2}{61} \right) = (-1)^{61-1/8} = -1.$$

Again by Reciprocity law .

$$\left(\frac{3}{61} \right) = \left(\frac{61}{3} \right) (-1)^{(2/2)(60/2)} = \left(\frac{1}{3} \right) = 1.$$

$$\left(\frac{7}{61} \right) = \left(\frac{61}{7} \right) (-1)^{(2/2)(60/2)} = \left(\frac{5}{7} \right).$$

$$\left(\frac{7}{5}\right) = (-1)^{(4/2)(6/2)} = \left(\frac{2}{5}\right)$$

Hence $\left(\frac{-42}{61}\right) = 1.$

2nd Method Also we can evaluate $\left(\frac{-42}{61}\right)$ as follows :

Since $-42 \equiv 19 \pmod{61}$

$$\begin{aligned} \left(\frac{-42}{61}\right) &= \left(\frac{19}{61}\right) = \left(\frac{61}{19}\right) = (-1)^{(19-1)(61-1)/4} = \left(\frac{61}{19}\right) \\ &= \left(\frac{4}{19}\right) = . \end{aligned}$$

Since $61 \equiv 4 \pmod{19}.$

7.5. THE JACOBI SYMBOL

Jacobi extended Legendre's symbol (a/p) for composite number and formed analogous results for the new Jacobi symbol. We define it as follows:

DEFINITION : Let $(P, Q) = 1$, $Q > 0$, Q odd, so that $Q = q_1 q_2 \dots q_s$ where the q_i 's are not necessarily distinct. The Jacobi symbol (P/Q) is defined by

$$(15) \quad \left(\frac{P}{Q}\right) = \prod_{i=1}^s \left(\frac{P}{q_i}\right)$$

where $\left(\frac{P}{q_i}\right)$ is Legendre symbol.

Remark : If Q is an odd prime then Jacobi symbol is same as Legendre symbol.

Clearly $(P/Q) = \pm 1$. But it is not true that

$$(P/Q) = 1$$

$\Rightarrow P$ is a quadratic residue modulo Q .

For example $(2/9) = 1$ but $x^2 \equiv 2 \pmod{9}$ has no solution.

THEOREM 19 : Suppose that Q and Q' are odd and positive and that $(PP', QQ') = 1$, then

$$(i) \left(\frac{P}{Q} \right) \left(\frac{P}{Q'} \right) = \left(\frac{P}{QQ'} \right)$$

$$(ii) \left(\frac{P}{Q} \right) \left(\frac{P'}{Q} \right) = \left(\frac{PP'}{Q} \right)$$

$$(iii) \left(\frac{P^2}{Q} \right) = \left(\frac{P}{Q^2} \right) =$$

$$(iv) \left(\frac{P' P^2}{Q' Q^2} \right) = \left(\frac{P'}{Q'} \right)$$

$$(v) P \equiv P' \pmod{Q} \Rightarrow \left(\frac{P'}{Q} \right) \left(\frac{P}{Q} \right)$$

PROOF : (i) follows from the definition of (P/Q) and

(ii) follows from the definition and from the properties of Legendre's symbol.

(iii) follows from (i) and (ii) so also (iv). For (v) we write $Q = q_1 q_2 \dots q_s$.

Then $P' \equiv P \pmod{q_j}$ so that $(P'/q_j) \equiv (P/q_j)$. Hence (v) follows from the definition.

THEOREM 20 : If Q is odd and $Q > 0$, then

$$(16) \left(\frac{-1}{Q} \right) = (-1)^{Q-1/2} \text{ and } \left(\frac{2}{Q} \right) = (-1)^{(Q^2-1)/8}.$$

PROOF : We have

$$\left(\frac{-1}{Q} \right) = \prod_{j=1}^s \left(\frac{-1}{q_j} \right) = \prod_{j=1}^s (-1)^{(q_j-1)/2}$$

$$= (-1)^{\sum_{j=1}^s (q_j-1)/2}.$$

If a and b are odd, then

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2} \right) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod{2}$$

and hence

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod{2}.$$

Applying this repeatedly we obtain

$$\sum_{j=1}^s \left(\frac{q_j-1}{2} \right) = \frac{1}{2} \sum_{j=1}^s q_j - 1 \equiv \left(\frac{Q-1}{2} \right) \pmod{2}.$$

Thus

$$\left(\frac{-1}{Q} \right) = (-1)^{Q-1/2}.$$

Similarly if a and b are odd, then

$$\frac{a^2b^2-1}{8} \left(\frac{a^2-1}{8} + \frac{b^2-1}{8} \right) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod{8}.$$

So we have

$$\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{(a^2b^2-1)}{8} \pmod{2}$$

$$\sum_{j=1}^s \frac{q_j^2-1}{8} = \frac{Q^2-1}{8} \pmod{2}.$$

and hence

$$\begin{aligned} \left(\frac{2}{Q} \right) &= \prod_{j=1}^s \frac{2}{q_j} = (-1)^{\sum_{j=1}^s (q_j^2-1)/8} \\ &= (-1)^{(Q^2-1)/8}. \end{aligned}$$

THEOREM 21 : If P and Q are odd and positive and if $(P, Q) = 1$, then

$$(17) \quad \left(\frac{P}{Q} \right) \left(\frac{Q}{P} \right) = (-1)^{((P-1)/2)((Q-1)/2)}.$$

PROOF : Writing $P = \prod_{i=1}^r p_i$ and $Q = \prod_{j=1}^r q_j$

$$\left(\frac{P}{Q}\right) = \sum_{j=1}^s \left(\frac{P}{q_j}\right) = \sum_{j=1}^s \sum_{i=1}^r \left(\frac{p_i}{q_j}\right)$$

$$= \left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) (-1)^{\sum_{j=1}^s \sum_{i=1}^r \{(p_i-1)/2\} \{(q_j-1)/2\}}$$

By theorem 15 we have

$$\sum_{j=1}^s \sum_{i=1}^r \frac{(p_i-1)}{2} \frac{(q_j-1)}{2} = \sum_{i=1}^r \frac{(p_i-1)}{2} \sum_{j=1}^s \frac{(q_j-1)}{2}$$

and

$$\sum_{i=1}^r \frac{p_i-1}{2} \equiv \frac{P-1}{2}, \sum_{j=1}^s \frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod{2}$$

and

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) (-1)^{\{(P-1)/2\} \{(Q-1)/2\}}$$

which proves the theorem.

For example

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1.$$

Example 1 : Determine whether 888 is a quadratic residue or non-residue of the prime 1999.

Solution : We have

$$\begin{aligned} \left(\frac{888}{1999}\right) &= \left(\frac{4}{1999}\right) \left(\frac{2}{1999}\right) \left(\frac{111}{1999}\right) \\ &= \left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right) \left(\frac{37}{1999}\right). \end{aligned}$$

We can calculate $(3/1999)$ and $(37/1999)$ by applying quadratic reciprocity law . Also we have by Jacobi symbol

$$\left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1.$$

Therefore 888 is a quadratic non-residue modulo 1999.

Example 2 : Evaluate $\left(\frac{595}{7657}\right)$.

Solution : $595 = 5 \times 7 \times 17$, $7657 = 13 \times 19 \times 31$.

Hence $(7657, 595) = 1$.

$$\begin{aligned}\left(\frac{595}{7657}\right) &= \left(\frac{7657}{595}\right) = \left(\frac{517}{595}\right) \left(\frac{595}{517}\right) = \left(\frac{28}{517}\right) \\ &= \left(\frac{2}{517}\right) \left(\frac{39}{517}\right) = (-1) \left(\frac{517}{39}\right) = (-1) \left(\frac{10}{39}\right) \\ &= (-1) \left(\frac{2}{39}\right) \left(\frac{5}{39}\right) = -\left(\frac{39}{5}\right) \\ &= -\left(\frac{1}{5}\right) = -1.\end{aligned}$$

7.6. COMPUTING SQUARE ROOTS MOD p .

Once we know that the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution, how do we find it? We describe an algorithm that is extremely fast in its search for a solution.

Case(i) If $p \equiv 3 \pmod{4}$ ie $p = 4n + 3$, the solution is simple.

For in this case $x = a^{n+1} = a^{(p+1)/4}$ is a solution to $x^2 \equiv a \pmod{p}$.

We verify this by

$$x^2 \equiv a^{2n+2} \equiv a^{2n+1} a \equiv a^{(p-1)/2} a \equiv 1 a \pmod{p}$$

since

$$a^{p-1/2} \equiv 1 \pmod{p} \text{ for a quadratic residue } a.$$

Case (ii) If $p \equiv 1 \pmod{4}$ we can have $p \equiv 1, 5 \pmod{8}$. If $p \equiv 5 \pmod{8}$ and 2 is quadratic nonresidue mod $p = 8k+5$, we can solve the congruence as follows:

2 is a quadratic residue modulo p when $p = 8k + 5$.

By Euler's criterion

$$a^{p-1/2} \equiv 1 \pmod{p}$$

\Rightarrow

$$(a^{p-1/2} - 1) \equiv 0 \pmod{p}$$

If

$$a^{p-1/4} \equiv 1 \pmod{p}$$

then $x \equiv a^{p+3/8} \pmod{p}$ is a solution otherwise
 $x \equiv 2a(4a)^{p-3/8} \pmod{p}$ is a solution.

If $p = 4n + 3$. We write $p-1 = 2s$ with s odd. Let $x = a^{n+1} = a^{(s+1)/2}$ is the solution to $x^2 \equiv a \pmod{p}$ because $(a^{(s+1)/2})^2 \equiv a^s a$ and $a^s \equiv 1 \pmod{p}$. with s odd.

We can not repeat this for $p \equiv 3 \pmod{4}$ as $p-1/2$ is even ie if we write $p-1 = 2s$, then $s+1/2$ is not an integer. We write $p-1 = 2^r s$, with s odd. Let us try $x = a^{(s+1)/2}$ and see how much it differs from a solution

$$x^2 \equiv a^{s+1} \equiv a^s a \pmod{p}.$$

Now both a and x^2 are quadratic residues. So a^s is also quadratic residue. Suppose we know an element z such that $z^2 \equiv a^s \pmod{p}$, then we can write

$$x^2 \equiv z^2 a \pmod{p} \text{ multiplying by the inverse of } z^2,$$

$$\text{we get } (x z^{-1})^2 \equiv a \pmod{p}$$

that is, we can solve $x^2 \equiv a \pmod{p}$ if we can solve $z^2 \equiv a^s \pmod{p}$

$$\text{To solve } z^2 \equiv a^s \pmod{p}$$

The $\text{ord}_p a^s \mid 2^{r-1}$ and if z is a solution then $\text{ord}_p(z) \mid 2^r$.

Then there are 2^r elements of order dividing 2^r , and z must be one of these. Since 2^r can be much smaller than p , to find the solution is simpler. We illustrate this by example.

Example : Solve $x^2 \equiv 2 \pmod{41}$.

We write $p-1 = 41-1 = 40 = 8 \cdot 5 = 2^3 \cdot 5$, so $r = 3$ and $s = 5$ (odd). To search for elements of order $2^3 = 8$, the most natural idea is to look for a primitive root g (which has order 40); then g^5 and all its powers will have orders dividing 8. Now 7 is a primitive root modulo 41, and $7^5 \equiv 38 \pmod{41}$ has order 8.

$$\text{Let } S = \{ 38, 38^2, 38^3, 38^4, 38^5, 38^6, 38^7, 38^8 \}$$

All the elements of S have order dividing 8, and S includes all elements of orders that divide 8, as there are eight elements of order dividing 8. We reduce S modulo 41 to get

$$S = \{ 38, 9, 14, 40, 3, 32, 27, 11 \}.$$

Now

$$2^5 \equiv 32 \equiv 38^6 \pmod{41} \text{ is in this set}$$

and our solution is

$$\begin{aligned} x &\equiv 2^{(5+1)/2} 38^{-6/2} \\ &\equiv 2^3 \cdot 38^{-3} \equiv 2^3 38^5 \pmod{41} \text{ (since } 38^{-3} \equiv 38^5 \pmod{41}) \\ &\equiv 8 \cdot 3 \equiv 24 \pmod{41}. \end{aligned}$$

So

$$x \equiv 24 \pmod{41} \text{ satisfies the congruence}$$

$$x^2 \equiv 2 \pmod{41}.$$

ANOTHER ALGORITHM FOR FINDING SQUARE ROOTS MODULO p .

Let p be an odd prime, and suppose that we know a quadratic non residue n .

Let a be an integer such that $(a/p) = 1$. We want to find an integer x such that

$$x^2 \equiv a \pmod{p}.$$

First write $p-1 = 2^r s$ where s is odd. Then compute n^s modulo p , and call that b . Next compute $a^{(s+1)/2} \pmod{p}$, and call that α ,

Claim : We claim that α is close to being a square root of a . Take the ratio α^2/a , we claim that we get 2^{r-1} th root of unity modulo p .

$$(a^{-1} \alpha)^{2^{r-1}} = a^{s \cdot 2^{r-1}} = a^{(p-1)/2} = (a/p) = 1.$$

We must then modify α by a suitable 2^r th root of unity to get an x such that x^2/a is 1. To do this we claim that b is a primitive root of 2^r th root of unity, which means that all the 2^r th root of unity are powers of b . To see this first we note that b is a 2^r th root of 1, because

$$b^{2^r} = n^{2^r s} = n^{p-1} = 1. \text{ If } b \text{ were not primitive, there would be a lower}$$

power (a divisor of 2^r) of b that gives 1. But then b would be an even power of a primitive 2^r -th root of unity, so would be a square. This is impossible because $(b/p) = (n/p)^s = -1$ (since s is odd and n is a non residue).

These b is a primitive 2^r -th root of unity. Next to find b^j , $0 < j < 2^r$, such that

$x = b^j \alpha$ gives the desired square root of a . Write j in binary form as $j = j_0 + 2j_1 + \dots + 2^{r-2} j_{r-2}$ and show how one successively determines whether j_0, j_1, \dots is 0 or 1. To find binary digits of j we have to proceed as follows.

1. Raise (α^2/a) to the 2^{r-2} -th power. The square of this is 1.

Hence we get either ± 1 . If we get 1 then $j_0 = 0$, if we get -1 , take $j_0 = 1$. We note that j_0 has been chosen so that

$$((b^{j_0} \alpha)^2/a) \text{ is a } 2^{r-2} \text{th root of unity.}$$

2. Suppose we have found j_0, j_1, \dots, j_{k-1}

such that $\left(\frac{b^{j_0+2j_1+\dots+2^{k-1}j_{k-1}}\alpha}{a} \right)^2$ is 2^{r-k-1} th root of unity and we

want to find j_k . Raise this number to half the power that gives 1, and choose j_k according to whether you get +1 or -1

$$\text{if } \left(\frac{\left(\frac{b^{j_0+2j_1+\dots+2^{k-1}j_{k-1}}\alpha}{a} \right)^2 \right)^{2^{r-k-1}} = \begin{cases} 1 \\ -1 \end{cases}$$

then take $j_k = \begin{cases} 0 \\ 1 \end{cases}$, respectively.

i.e. $\left(\frac{b^{j_0+2j_1+\dots+2^k j_k} \alpha}{a} \right)^2$ is a 2^{r-k-2} th root of unity.

when we get $k \equiv r-2$ and find j_{r-2} , we then have

$$\left(\frac{b^{j_0+2j_1+\dots+2^{r-2}j_{r-2}}\alpha}{a} \right)^2 = 1.$$

Example : Find square root of $a = 186 \pmod{p}$; $p = 401$ i.e. to solve $x^2 \equiv 186 \pmod{401}$ using the above algorithm.

Solution : The first non residue is $n = 3$. we have $p-1 = 400 = 2^4 \cdot 25$, and so

$$b = 3^{25} = 268 \text{ and}$$

$$\alpha = a^{13} = (186)^{13} \equiv 103 \pmod{401}.$$

Compute $a^{-1} = (186)^{-1} = 235 \pmod{401}$, $\alpha^2/a = 98$, which must be an 8^{th} root of unity. Compute 98^4 . Since $98^4 \equiv -1 \pmod{401}$ and so $j_0 = 1$.

Next we compute $(b\alpha)^2/a = -1$.

Since the 2^{nd} power of this is 1, we have $j_1 = 0$ and hence $j_2 = 1$.

Thus $j = 5$ and the desired square root is $b^5 \alpha = 304$.

7.7. APPLICATION TO CRYPTOGRAPHY

We have studied public key cryptography. For identification a signature attached to a message can be used to verify the sender's identity. In many applications, it is necessary to verify the identity of the sender before a message is sent. For example we use a Personal Identification Number or PIN to conduct many transactions. Telephone calling cards, and credit cards use a PIN to validate transactions.

Suppose Amit is using a PIN as a secret key to access some services. Someone looking over his shoulder or eavesdropping electronically can receive his PIN and impersonate Amit. Identification schemes are designed to protect against security problems that arise when a secret key is compromised. Instead of revealing the secret key to verify Amit's identity, these schemes provide a mechanism for Amit to prove that he knows the secret key. A proof of identity is based on some computation involving this key and the intermediate results of computation are different for each identification session.

Now one of the identification schemes is based on the difficulty of factoring integers. Let $n = pq$, where p and q are primes. Solving quadratic congruence modulo n is equivalent to computing the prime factorization of n . Suppose a is a quadratic residue modulo n . If we know the prime factorization of n , then we can solve the congruence $x^2 \equiv a \pmod{n}$ by solving $x^2 \equiv a \pmod{p}$ and $x^2 \equiv a \pmod{q}$. Conversely we can compute the four roots of $x^2 \equiv a \pmod{n}$ then we can factor n . If the roots are $\pm x_0$ and $\pm y_0$ then $x_0^2 \equiv y_0^2 \pmod{n}$ but $x_0 \not\equiv \pm y_0 \pmod{n}$, so $(x_0 - y_0, n)$ is a proper factor of n .

In this identification scheme due to Feige-Fiat-Shamir, the number $n = pq$ can be shared among a group of users, without their knowing p and q . A trusted central authority can assign n and public and private keys based on n . We require $(v, n) \neq 1$. Amit's private key is number s , $0 < s < n$, such that

$$s^2 \equiv v^{-1} \pmod{n}.$$

The protocol for Amit to prove his identity to Bobby consists of the following steps. Bobby knows the number n and Amit's public key v .

1. Amit selects a random number r , $0 < r < n$ and sends $x = r^2 \pmod{n}$ to Bobby
2. Bobby selects a random bit, $b = 0$ or 1 and sends b to Amit.
3. If $b = 0$, then Amit returns r to Bobby, otherwise, Amit returns $y = (rs) \pmod{n}$.

4. If $b = 0$, then Bobby verifies that $x = r^2 \pmod{n}$ and if $b = 1$, then Bobby verifies that $y^2 \equiv x v^{-1} \pmod{n}$.

Verification : Amit's identity is verified because he is proving his knowledge of the private key s , without revealing it. This protocol is repeated many times to validate Amit's identity. This scheme is secure, because if a third person Anu is trying to impersonate Amit without knowing s satisfying $s^2 \equiv v^{-1} \pmod{n}$, then Anu cannot satisfy both the condition in step 4. If he sends x such that $x = r^2 \pmod{n}$, then he can not find $y^2 \equiv x v^{-1} \pmod{n}$ without knowing prime factors of n . If he chooses x and y such that $y^2 \equiv x v^{-1} \pmod{n}$, then he will be able to satisfy the quarry when $b = 1$ but not when $b = 0$. If b is randomly chosen bit, the probability that Anu can guess it correctly in advance is $1/2$. If the protocol is repeated k times, the probability that Anu has guessed each bit correctly is $1/2^k$. So if k is chosen to be large value, say $k \geq 50$, then the chance of some one impersonality Amit are slim.

THEOREM 22 : Suppose x is a quadratic residue modulo $n = pq$, with p and q primes satisfying $p \equiv q \equiv 3 \pmod{4}$. Then there is a unique y such that $y^2 \equiv x \pmod{n}$ and y is a quadratic residue modulo n .

PROOF : Since n is a product of two primes, there are four solutions to the congruence $y^2 \equiv x \pmod{n}$. If y_0 is a solution, then the four solutions are

$$\begin{array}{ll} y \equiv y_0 \pmod{p} & y \equiv y_0 \pmod{p} \\ y \equiv y_0 \pmod{q} & y \equiv -y_0 \pmod{q} \\ y \equiv -y_0 \pmod{p} & y \equiv -y_0 \pmod{p} \\ y \equiv y_0 \pmod{q} & y \equiv -y_0 \pmod{q}. \end{array}$$

The four possible solutions give rise to four possible combinations of the Legendre symbol (y/p) and (y/q) . The four pairs are:

$$\{(y_0/p), (y_0/q), (y_0/p), (-y_0/q)\}, \\ (-y_0/p), (y_0/q), (-y_0/p), (-y_0/q)$$

Since $p \equiv q \equiv 3 \pmod{4}$, the Legendre symbols $(-1/p)$ and $(-1/q)$ are both -1 , and each of the four possible combinations of signs. $\{1, 1\}$, $\{1, -1\}$, $\{-1, 1\}$ and $\{-1, -1\}$ must occur once, irrespective of the values of (y_0/p) and (y_0/q) . Hence, there is only one y such that $(y/p) = 1$ and $(y/q) = 1$, that is there is only one solutions to $y^2 \equiv x \pmod{n}$ such that y is a quadratic residue modulo n .

Example : Consider $n = pq$ with $p = 331$ and $q = 431$. We select $x = 11535$ as a quadratic residue modulo n we can solve $y^2 \equiv x \pmod{n}$, to obtain the solutions $y \equiv \pm 127060, \pm 58962 \pmod{n}$. Of these four, only one, 127060 is a quadratic residue modulo n .

As an application to cryptography to construct a one-time pads in a public key system. A onetime pad is a string $s_0, s_1, s_2 \dots s_k$ that is added to the plaintext $p_0, \dots p_k$ to produce a ciphertext $c_0, c_1, \dots c_k$. This is represented by $c_i = p_i + s_i \pmod{2}$. Suppose Amit set a public key $n = pq$, where p and q satisfy $p \equiv q \equiv 3 \pmod{4}$. If Bobby wishes to send a coded message to Amit, then he chooses a number x_0 and compute the sequence $x_0, x_1 \dots x_k x_{k+1}$ where $x_{i+1} \equiv x_i^2 \pmod{n}$ for $i = 0, 1, 2, \dots k$ then Bobby compute the bits $s_i = x_i \pmod{2}$. The random bit stream $s_1, s_2, \dots s_k$ is used as one time pad to the plaintext $p_1, p_2, \dots p_k$.

Bobby sends the ciphertext $c_0, c_1 \dots c_k$ with $c_i = p_i + s_i \pmod{2}$ and the integer x_{k+1} . Amit uses x_{k+1} to recover the number $x_k, x_{k-1}, \dots x_1$ and from this, the one time pad. It is easy to recover the plaintext from the knowledge of the ciphertext and the one time pad.

The scheme works because there is only one square root of each term that is a quadratic residue. The scheme is more secure as it depends on computing y satisfying $y^2 \equiv x \pmod{n}$ is equivalent to factoring n .

EXERCISES

1. Prove that $\sum_{j=1}^{p-1} (j/p) = 0$, p an odd prime.
2. Evaluate (i) $\left(\frac{-25}{83}\right)$ (ii) $\left(\frac{-23}{83}\right)$ (iii) $\left(\frac{51}{79}\right)$
(iv) $\left(\frac{71}{73}\right)$ (v) $\left(\frac{105}{73}\right)$ (vi) $\left(\frac{-35}{97}\right)$.
3. Prove that if p and q are distinct prime of the form $4k + 3$, and if $x^2 \equiv p \pmod{q}$ has no solution, then $x^2 \equiv q \pmod{p}$ has two solutions.
4. Show that 665 is a quadratic residue of 1443.
5. Find the solutions of $x^{78} \equiv 1 \pmod{13}$.
6. Let p be an odd prime prove each of the following statements:

$$(i) \sum_{r=1}^{p-1} r \left(\frac{r}{p}\right) = 0 \text{ if } p \equiv 1 \pmod{4}.$$

$$(ii) \sum_{r=1}^{p-1} r = \frac{p(p-1)}{4} \text{ if } p \equiv 1 \pmod{4}.$$

$$\left(\frac{r}{p}\right) = 1$$

$$(iii) \quad \sum_{r=1}^{p-1} r^2 (r/p) = p \sum_{r=1}^{p-1} r (r/p) \text{ if } p \equiv 3 \pmod{4}.$$

$$(iv) \quad \sum_{r=1}^{p-1} r^3 (r/p) = 3/2 p \sum_{r=1}^{p-1} r^2 (r/p) \text{ if } p \equiv 1 \pmod{4}.$$

$$(v) \quad \sum_{r=1}^{p-1} r^4 (r/p) = 2p \sum_{r=1}^{p-1} r^3 (r/p) - p^2 \sum_{r=1}^{p-1} r^2 (r/p)$$

if $p \equiv 3 \pmod{4}$.

7. Prove that if $p \equiv 3 \pmod{4}$

$$\{(2/p) - 2\} \sum_{r=1}^{p-1} r (r/p) = p \sum_{r=1}^q (r/p)$$

where $q = p-1/2$.

8. Prove that 3 is a quadratic non residue of all primes of the form $2^{2n} + 1$, as well as primes of the form $2^p - 1$, where p is a prime.
9. Determine whether the following quadratic congruences are solvable.
 - (a) $x^2 \equiv 219 \pmod{419}$.
 - (b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$.
 - (c) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$.
10. Evaluate the Jacobi symbols
 - (a) $\left(\frac{21}{221}\right)$
 - (b) $\left(\frac{215}{253}\right)$
 - (c) $\left(\frac{631}{1099}\right)$
11. Use Gauss lemma to show that 17 is a quadratic residue modulo 19.
12. Does the congruence $x^2 \equiv 631 \pmod{1093}$ has any solution ?
13. Show that $x^2 \equiv 15 \pmod{89}$ has no solution.
14. Write a computer program to evaluate Legendre symbol (a/p) using Euler's criterion.
15. Show that the smallest positive quadratic non-residue modulo p is always a prime.



PRIMALITY TESTING AND FACTORING

8.1. PSEUDOPRIMES AND CARMICHAEL NUMBERS

As an application of number theory to cryptography we want to know if large number n is prime. For example, we have shown in chapter v that in the RSA public key cryptosystem we need to find a large “random” prime. For this we use primality testing which means to determine whether an integer of a certain very special type is a prime.

PRIMALITY TEST : A primality test is a criterion for a number n not to be prime. If n ‘passes’ a primality test, then it may be prime. If it passes a whole lot of primality tests, then it is very likely to be prime. If n fails any single primality test then n is surely composite. But if n is composite and large enough then it is difficult to factorize it. In this chapter we will study some primality test and factorization of big primes.

The simplest primality test is “trial division”. Suppose n is a large odd integer. To test whether or not n is prime. Take an odd integer m and see whether or not it divides n . If $m \neq 1$, and $m \mid n$, then n is composite otherwise n passes the primality test “trial division by m ”. If n passes all the trial division test then n is prime. We know that n is prime when m reaches \sqrt{n} . Of course this trial division method is very time consuming. We will search for other test. One is the Fermat’s little theorem Fermat’s theorem tells that if $\gcd(b, n) = 1$ for any b and n is prime then

$$(1) \quad b^{n-1} \equiv 1 \pmod{n}.$$

If n is not prime it is still probable that (1) holds. We define pseudoprime as follow:

DEFINITION : If n is an odd composite number and b is an integer such that

$\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$ then n is called as the pseudoprime to the base b .

We say that 'pseudoprime' is a number n that 'pretends' to be prime by passing the test (1).

Example 1 : $n = 91$ is a pseudoprime to the base $b \equiv 3$, because

$$\gcd(3, 91) = 1 \quad \text{and}$$

$$3^{90} \equiv 1 \pmod{91}.$$

But 91 is not a pseudoprime to the base 2, because $2^{90} \equiv 64 \pmod{91}$.

But 91 is composite and

$$2^{90} \not\equiv 1 \pmod{91}.$$

Therefore 91 is not a pseudoprime to the base 2.

Example 2 : 15 is a pseudoprime to the base 4 and 11 but not to the base 2 and 3.

We have to show that

$$4^{14} \equiv 1 \pmod{15}$$

$$\text{Since } 4^2 \equiv 1 \pmod{15}$$

$$\Rightarrow 4^{14} \equiv 1 \pmod{15}$$

$$11^{14} \equiv 1 \pmod{15} \text{ since } 11^2 \equiv 1 \pmod{5},$$

$$11^2 \equiv 1 \pmod{3}$$

$$\text{Hence } 11^2 \equiv 1 \pmod{15}$$

$$\Rightarrow (11)^{14} \equiv 1 \pmod{15}.$$

$$\text{But } 2^{14} \not\equiv 1 \pmod{15} \text{ and } 3^{14} \not\equiv 1 \pmod{15}.$$

THEOREM 1 : Let n be an odd composite integer. Then

- (a) n is pseudoprime to the base b , where $\gcd(b, n) = 1$, if and only if the order of b divides $n-1$.
- (b) If n is pseudoprime to the bases b_1 and b_2 where $\gcd(b_1, n) = 1$ and $\gcd(b_2, n) = 1$, then n is a pseudoprime to the base $b_1 b_2$ and also to the base $b_1 b_2^{-1}$.
- (c) If n fails the test (1) for a single base b , then n fails (1) for at least half of the possible bases.

PROOF : To prove (a): From the hypothesis we have $b_1^{n-1} \equiv 1 \pmod{n}$ and

$$b_2^{n-1} \equiv 1 \pmod{n}.$$

These two imply $(b_1 b_2)^{n-1} \equiv 1 \pmod{n}$. This proves (a).

Similarly the proof of (b) follows. To prove (c), let $\{b_1, b_2, \dots, b_s\}$ be the set of all bases for which n is pseudoprime, i.e. the set of all integers $0 < b_i < n$ for which the congruence (1) holds. Let b be a fixed base for which n is not a pseudoprime. If n were pseudoprime for any of the bases $b b_i$, then by (b) it would be a pseudoprime for the base $b \equiv (b b_i) b_i^{-1} \pmod{n}$ which is not the case. Thus, for the s distinct residues $\{b b_1, b b_2, \dots, b b_s\}$, the integer n fails the test (1). Hence, there are at least as many bases for which n fails to be a pseudoprime as there are base for which (1) holds. Hence proved.

Now the question is: For a composite n (1) holds for every b ?

The answer is yes, and such a number is called a Carmichael number. Such numbers first studied by R. D. Carmichael in 1912. We define Carmichael number as follows :

DEFINITION 2 : A Carmichael number is a composite integer n such that

$$(2) \quad b^{n-1} \equiv 1 \pmod{n} \text{ for every } b.$$

Example : 561 is the smallest Carmichael number.

561 is composite as $561 = 3 \cdot 11 \cdot 17$. To show that $a^{560} \equiv 1 \pmod{561}$. By Fermat's theorem

$$\begin{aligned} & a^2 \equiv 1 \pmod{3} \\ \Rightarrow & a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3} \\ & a^{10} \equiv 1 \pmod{11} \\ \Rightarrow & a^{560} \equiv 1 \pmod{11} \quad (a^{10})^{56} \equiv 1 \pmod{11}. \\ & a^{16} \equiv 1 \pmod{17} \\ \Rightarrow & a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Since 3, 11, 17 are mutually relatively prime we obtain

$$a^{560} \equiv 1 \pmod{561} \text{ for all } a.$$

Example 2 : 341 is not a Carmichael number.

$$341 = 11 \times 31$$

$$\begin{array}{ll} a^{10} \equiv 1 \pmod{11} & a^{30} \equiv 1 \pmod{31} \\ (a^{10})^{34} \equiv 1 \pmod{11} & a^{340} \equiv 1 \pmod{31} \\ a^{340} \equiv 1 \pmod{11} & \text{So } a^{340} \equiv 1 \pmod{341} \end{array}$$

PROPERTIES OF CARMICHAEL NUMBERS

THEOREM 2 : A composite number n is a Carmichael number if and only if for every $p|n$ we have that $p-1|n-1$.

PROOF : First suppose that $p-1|n-1$ for every p dividing n . Let 3 be any base, where $\gcd(b, n) = 1$. Then for every p dividing n we have b^{n-1} is a power of b^{p-1} , and so is $\equiv 1 \pmod{p}$. These $b^{n-1} - 1$ is divisible by all prime factors p of n , and hence by their product which is n . Hence (2) holds. Conversely, suppose that there is a p such that $p-1 \nmid n-1$. Let g be an integer which is a generator. Find an integer b which satisfies $b \equiv g \pmod{p}$ and $b \equiv 1 \pmod{n/p}$. Then $\gcd(b, n) = 1$, and $b^{n-1} \equiv g^{n-1} \pmod{p}$. But $g^{n-1} \not\equiv 1 \pmod{p}$ because $(n-1)$ is not divisible by the order $p-1$ of g . Hence $b^{n-1} \not\equiv 1 \pmod{p}$ and so (2) can not hold. This completes the proof of the theorem.

THEOREM 3 : Let n be a composite integer. If n is divisible by a perfect square > 1 then n is not a Carmichael number.

PROOF : Suppose that $p^2|n$. Let g be a generator modulo p^2 , i.e. an integer such that $g^{p(p-1)}$ is the lowest power of g which is congruent to 1 mod p^2 . Let n' be the product of all primes other than p which divide n . By the Chinese Remainder theorem, there is an integer b satisfying the congruence.

$$b \equiv g \pmod{p^2} \text{ and } b \equiv 1 \pmod{n'}$$

Then b is, like g , a generator modulo p^2 , and it satisfies $\gcd(b, n) = 1$, since it is not divisible by p or by any prime which divides n' . n is not a pseudoprime to the base b . If (2) holds, then since $p^2|n$, we have $b^{n-1} \equiv 1 \pmod{p^2}$. But in that case $p(p-1)|n-1$, since $p(p-1)$ is the order of $b \pmod{p^2}$. However $n-1 \equiv -1 \pmod{p}$ since $p|n$ and this gives that $n-1$ is not divisible by $p(p-1)$. This contradiction proves that there is a base b for which n fails to be a pseudoprime.

THEOREM 4 : A Carmichael number is the product of at least three distinct primes.

PROOF : Suppose $n = pq$ the product of two distinct primes. Suppose that $p < q$.

Then, if n were a Carmichael number, we would have $n-1 \equiv 0 \pmod{q-1}$.

But $n-1 = p(q-1+1)-1 \equiv p-1 \pmod{q-1}$ and this is not $\equiv 0 \pmod{q-1}$, since $0 < p-1 < q-1$. This completes the proof.

Example 1 : 561 is a Carmichael number since $n = 561 = 3 \cdot 11 \cdot 17$ and 560 is divisible by $3-1$, $11-1$ and $17-1$.

Example 2 : $1105 = 5.13.17$ is a Carmichael number since 1104 is divisible by 4, 12 and 16.

8.2. STRONG PSEUDOPRIMES AND PROBABILISTIC PRIMALITY TESTING.

We define strong pseudoprimes as follow :

DEFINITION 1 : Let n be an odd composite number, and write $n-1 = 2^s t$ with t odd. Let b be any integer. If n and b satisfy the condition either $b^t \equiv 1 \pmod{n}$ or there exist r , $0 \leq r < s$, such that $b^{2^r t} \equiv -1 \pmod{n}$, then n is called a strong pseudoprime to the base b .

DEFINITION 2 : Let n be an odd integer, and let (b/n) denote the Jacobi symbol. If n is a prime number, then

$$(3) \quad b^{(n-1)/2} \equiv (b/n) \pmod{n}.$$

DEFINITION 3 : If n is an odd composite number and b is an integer such that $\gcd(n, b) = 1$ and (3) holds, then n is called a Euler pseudoprime to the base b .

THEOREM 5 : if n is a Euler pseudoprime to the base b , then it is pseudoprime to the base b . But the converse is not true.

PROOF : If n is a Euler pseudoprime to the base b , by definition

$$b^{(n-1)/2} \equiv (b/n) \pmod{n}, \quad \gcd(n, b) = 1.$$

Squaring both sides of the congruence we have

$$b^{n-1} \equiv 1 \pmod{n}; \quad \gcd(n, b) = 1.$$

Which implies n is a pseudoprime to the base b .

The converse is not true can be shown by the following example .

Example : 91 is a pseudoprime to the base 3. However $3^{91-1/2} \equiv 27 \pmod{91}$ so (3) is not true for $n = 91$ and $b = 3$. Hence 91 is not Euler pseudoprime to the 3. But 91 is a pseudoprime to the base 10, since $10^{91-1/2} = 10^{45} \equiv 10^3 \equiv -1 \pmod{91}$ and since

$$\left(\frac{10}{91}\right) = \left(\frac{2}{91}\right) \left(\frac{5}{91}\right).$$

$$\left(\frac{2}{91}\right) = (-1)^{(91)^2-1/8} = -1.$$

$$\left(\frac{5}{91}\right) = \left(\frac{91}{5}\right) (-1)^{(5-1)(91-1)/4} = \left(\frac{91}{5}\right) = \left(\frac{1}{5}\right) =$$

Hence $\left(\frac{10}{91}\right) = -1.$

So $10^{45} \equiv \left(\frac{10}{91}\right) \pmod{91}.$

THEOREM 6 : If $n \equiv 3 \pmod{4}$, then n is strong pseudoprime to the base b if and only if it is an Euler pseudoprime to the base b .

PROOF : Since $n \equiv 3 \pmod{4}$ i.e. $n = 4k + 3$,

here $n-1 = 4k + 2 = 2(2k+1)$

Hence $s = 1$ and $t \equiv n-1/2$.

We see that n is a strong pseudoprime to the base b if and only if

$b^{(n-1)/2} \equiv \pm 1 \pmod{n}$. If n is a Euler pseudoprime then the congruence holds by definition. Conversely suppose that $b^{n-1/2} \equiv \pm 1$. To show that ± 1 on the right is the Jacobi symbol (b/n) .

But for $n \equiv 3 \pmod{4}$ i.e. $n = 4k + 3$, $\pm 1 = (\pm 1/n)$, and so

$$\begin{aligned} \left(\frac{b}{n}\right) &= \left(\frac{b(b^2)^{n-3/4}}{n}\right) = \left(\frac{b^{n-1/2}}{n}\right) \\ &\equiv b^{n-1/2} \pmod{n}. \end{aligned}$$

Hence $b^{n-1/2} \equiv (b/n) \pmod{n}$.

Hence n is Euler pseudoprime. This completes the proof of the theorem.

THEOREM 7 : If n is a strong pseudoprime to the base b , then it is an Euler pseudoprime to the base b .

The proof is difficult and lengthy. We are leaving it.

THEOREM 8 : If n is an odd pseudoprime to the base 2, then the Mesenne number $2^n - 1$ is a strong pseudoprime to the base 2.

PROOF : First we will prove that $2^n - 1$ a pseudoprime to the base 2.

Let $n^1 = 2^n - 1$.

To show that

$$2^{n^1} - 1 \equiv 1 \pmod{n^1} \text{ or } 2^{n^1} \equiv 2 \pmod{n^1}.$$

n is a 2 pseudoprime implies

$$2^{n-1} \equiv 1 \pmod{n} \text{ or } 2^n \equiv 2 \pmod{n}$$

$$\text{or} \quad n \mid 2^n - 2 = n^1 - 1.$$

$$\begin{aligned} \Rightarrow \quad n^1 - 1 &= nk \text{ for some } k, \text{ then } 2^{n^1-1} - 1 = 2^{nk} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + \dots + 2^n + 1), \\ &= n^1 (2^{n(k-1)} + \dots + 2^n + 1) \end{aligned}$$

$$\Rightarrow \quad n^1 \mid 2^{n^1-1} - 1 \text{ or } 2^{n^1-1} \equiv 1 \pmod{n^1}$$

$$\text{or} \quad 2^{n^1} \equiv 2 \pmod{n^1} \text{ the required result.}$$

Next to show that $2^n - 1$ is a strong pseudoprime to the base 2.

We write $n^1 - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk$, so the odd part of $n^1 - 1$ is nk .

Clearly $2^n - 1 \equiv 0 \pmod{2^n - 1}$ or $2^n \equiv 1 \pmod{n^1}$.

This implies that $2^{nk} \equiv 1 \pmod{n^1}$ since nk is odd part of $n^1 - 1$, this shows that

$n^1 = 2^n - 1$ is a strong pseudoprime to the base 2 This completes the proof.

ALGORITHM 1 : (Simple primality Test)

Given $n \leq 25.10^9$, this algorithm determines if n is prime.

1. If n fails the strong pseudoprime test to base 2, then n is composite.
2. If n fails strong pseudoprime test to base 3, then n is composite
3. If n fails the strong pseudoprime test to base 5, then n is composite.
4. If n fails the strong pseudoprime test to the base 7 then n is composite.
5. If n fails strong pseudoprime test to the base 11 then n is composite.

Example : Consider $n = 117371$. We factorize $n-1 = 2.58685$.

Compute

$$2^t \equiv -1 \pmod{n} \text{ where } t = 58685,$$

$$\text{and} \quad 2^{2t} \equiv 1 \pmod{n}$$

$$\text{and} \quad 3^t \equiv 1 \pmod{n} \text{ where } t = 58685.$$

This implies n is strong pseudoprime

Note : It is to note that the strong pseudoprimes are much more useful than pseudoprimes to detect compositeness.

If n fails a strong pseudoprime test, then it is composite. Suppose we check for 50 random bases, then the probability that a composite number successfully passes 50 random pseudoprime test is less than $\frac{1}{2} 50$. In this case the number is very likely to be prime. We call a number that passes this test a **probable prime** we must note that this does not prove that the number is prime.

We are giving now the following probabilistic algorithm for compositeness, or detecting probable primes.

ALGORITHM 2 : (Rabin –Miller Probabilistic Primality Test)

We use the strong pseudoprime test to several random bases to check if n is a probable prime. The test should only be applied after checking if the number has any small factors.

1. [initialize] Let $t = n-1$, $s = 0$, $k = 50$
2. [Compute $n-1 = 2^s \cdot t$]. If $t \equiv 0 \pmod{2}$, $t = t/2$, $s = s + 1$, and repeat step 2. Otherwise go to step 3.
3. Choose a random integer $b < n$ and set $b = b^t \pmod{n}$ and $c = 0$. if $b = 1$. go to step 5, otherwise go to step 4.
4. If $c > s-2$ or $b = 1$, then n is composite. If $b = -1$ go to step 5 otherwise
 $b = b^2 \pmod{n}$, $c = c + 1$, repeat step 4.
5. Let $k = k-1$. If $k > 0$, go to step 3. Otherwise, report that n is a probable prime.

Probabilistic primality tests are quite sufficient for large primes. We give now a short and easy primality test to verify whether n is prime or composite.

We have defined earlier the order and primitive root of an integer mod n .

8.3. PRIMALITY TESTING (APPLICATION OF PRIMITIVE ROOTS AND INDICES TO CRYPTOGRAPHY)

Now we will give Lucas–Lehmer primality test and the ElGamal Cryptosystem.

THEOREM 9 : (Lucas Lehmer) Suppose there exists an integer b such that

$b^{n-1} \equiv 1 \pmod{n}$. But for each prime q dividing $n-1$, $b^{(n-1)/q} \not\equiv 1 \pmod{n}$, then n is prime.

PROOF : To prove that $\text{ord}_n(b) = n-1$. The congruence $b^{n-1} \equiv 1 \pmod{n}$

$$\Rightarrow \text{ord}_n(b) \mid n-1.$$

Let $n-1 = \text{ord}_n(b) \cdot k$ for some k . To show that $k = 1$, so suppose that $k > 1$ and a prime q divide k , then $q \mid n-1$, and we can write

$$b^{(n-1)/q} = b^{(\text{ord}_n(b) \cdot k)/q} \equiv 1 \pmod{n}.$$

This contradicts the hypothesis of the theorem, so $k = 1$ and $\text{ord}_n(b) = n-1$.

As $\text{ord}_n(b) \mid \phi(n)$, we must have $\phi(n) \geq n-1$, but $\phi(n) \leq n-1$, therefore $\phi(n) = n-1$ and n is prime.

Example 1 : Consider $n = 29$. $n-1 = 28 = 2^2 \cdot 7$

Take

$b = 2$. Now

$$2^{n-1} = 2^{28} \equiv 1 \pmod{29}$$

$$2^{28/2} = 2^{14} \equiv 28 \pmod{29}$$

i.e.

$$2^{14} \not\equiv 1 \pmod{29}$$

$$2^{28/7} = 2^4 \equiv 16 \pmod{29} \not\equiv 1 \pmod{29}$$

So by theorem 9, 29 is prime.

Example 2 : Let $n = 911$.

$$n - 1 = 910 = 2 \cdot 5 \cdot 7 \cdot 13$$

Now

$$7^{n-1} \equiv 1 \pmod{n}$$

$$7^{(n-1)/2} \equiv -1 \pmod{n}$$

$$3^{n-1} \equiv 1 \pmod{n}$$

$$3^{(n-1)/5} \equiv 482 \pmod{n}$$

$$2^{n-1} \equiv 1 \pmod{n}$$

$$2^{(n-1)/7} \equiv 568 \pmod{n}$$

$$2^{n-1} \equiv 1 \pmod{n}$$

$$2^{(n-1)/13} \equiv 1 \pmod{n}.$$

The ElGamal system (Application of Discrete logarithm to Cryptography).

The ElGamal system, a publickey cryptosystem, is based on the presumed difficulty of discrete logarithm problem. We know that if $r^x \equiv y \pmod{p}$ then x is the discrete logarithm of $y \pmod{p}$. There is no method to compute x with the knowledge of r , y and p , where p is a large prime.

The ElGamal system can be used for both encryption and signatures. We will describe the method as follows:

Suppose Ajit wishes to receive encrypted message. He chooses a prime p and a primitive root r modulo p . He selects a private key a , $0 < a < p-1$, and computes $b = r^a \pmod{p}$. Ajit's public key is $k = (r, b, p)$. To encrypt a message m , $0 < m < p$, one has to proceed as follows :

1. Choose a random number s , $1 < s < p-1$
2. compute $y_1 = r^s \pmod{p}$ and $y_2 = m b^s \pmod{p}$.
3. The ciphertext is $E_K(m) = (y_1, y_2)$.

The security lies in the choice of random number r . Ajit can recover m using the decryption function

$$D_k(y_1, y_2) = y_2 (y_1)^{-a} \pmod{p}.$$

This is valid because

$$\begin{aligned}
 D_k(y_1, y_2) &= y_2 (y_1)^{-a} \bmod p \\
 &= y_2 (r^{-sa}) \bmod p \\
 &= y_2 (r^a)^{-s} \bmod p \\
 &= m b^s b^{-s} \bmod p \\
 &= m \bmod p.
 \end{aligned}$$

Example : Let $p = 37$, $r = 2$ and $a = 31$.

Then $b = 2^{31} \bmod 37 = 22$. Suppose plaintext is $m = 19$. Let A chooses a random number say $s = 7$; then

$$\begin{aligned}
 y_1 &= 2^7 \bmod 37 \\
 &\equiv 17, \\
 y_2 &\equiv 19 \cdot 22^7 \bmod 37 \\
 &\equiv 19 \cdot 2 \bmod 37 \\
 &\equiv 1.
 \end{aligned}$$

Then A sends $E_K(m) = (17, 1)$ to B. To decipher this B computes $D_K(17, 1)$

$$= 17^{-31} \bmod 37 = 19.$$

The security of the system lies in the computation of the private key a from the public key parameters using discrete logarithm problem, which is difficult. Hence the security of the ElGamal system is equivalent to the discrete log problem.

Another quality of the system which is important for its security is the choice of random number s . The same value of s should not be used with different plaintext. If the same s is used for different plaintext, then it will be possible to recover all plaintext from the knowledge of one.

In the subsequent section we will discuss some factorization method.

8.4. POLLARD'S (p-1) METHOD

We discuss two factorization method due to J. N. Pollard. Pollard's (p-1) methods is the following :

Suppose n is the number to be factored, and say $p|n$, p is a prime.

Now $b^{p-1} \equiv 1 \pmod{p}$ for any b such that $\gcd(b, p) = 1$.

Suppose $p-1$ divides a number M ; then $a^M \equiv 1 \pmod{p}$ ie $p|a^M - 1$.

Since $p|n$ and $p|a^M - 1$, p will divide their $\gcd(n, a^M - 1)$.

We compute $a^{M-1} \pmod{n}$ and $(a^{M-1} \pmod{n}, n)$. If this gcd is not equal to n , then we would have found a non trivial factor of n . This factor is p . Let us illustrate by example.

Example 1 : Consider $n = 1073 = 29 \cdot 37$. If $p = 29$, $p-1 = 28$. Let $b = 2$
 $2^{28} \equiv 900 \pmod{1073}$ and $(900 - 1, 1073) = 29$.

Similarly

$$2^{36} \equiv 777 \pmod{1073}$$

and $(777 - 1, 1073) = 37$, the second factor.

8.5. POLLARD'S RHO METHOD

The first step in this method is to choose an easily evaluated map from $\mathbb{Z}/n\mathbb{Z}$ to itself, a simple polynomial with integer coefficients such as $f(x) = x^2 + 1$. Next choose a particular value $x = x_0$ ($x_0 = 1$ or 2 or randomly generated integer) and compute the successive iterates of f : $x_1 = f(x)$, $x_2 = f(f(x_0))$, $x_3 = f(f(f(x_0)))$.

We define $x_{j+1} = f(x_j)$ $j = 0, 1, 2, \dots$

Compare between different x_j 's, find two which are in different residue classes modulo n but in the same residue classes modulo some divisor of n .

Finding such x_j, x_k , we have $\gcd(x_j - x_k, n)$ is equal to a proper divisor of n , and complete the factorization.

Example 1 : Factor 91 choosing $f(x) = x^2 + 1$, $x_0 = 1$.

We have $x_1 = f(x_0) = 2$

$$x_2 = 5, x_3 = 26$$

We find $\gcd(x_3 - x_2, n) = \gcd(21, 91) = 7$, so 7 is a factor.

Exercise : Factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$.

8.6. FERMAT'S FACTORIZATION METHOD

Fermat factorization is based on the fact that n is equal to difference of two squares, one of which is very small.

THEOREM 10 : Let n be a positive odd integer. There is 1 to 1 correspondence between factorization of n in the form $n = ab$, where $a \geq b > 0$, and representation of n in the form $t^2 - s^2$, where s and t are non negative integers. The correspondence is given by the equation .

$$t = a+b/2, s = a-b/2, a = t+s, b = t-s.$$

PROOF : We can write

$$n = ab = ((a+b)/2)^2 - ((a-b)/2)^2,$$

So we obtain the representation as a difference of two square.

Conversely, given $n = t^2 - s^2$, we can write $n = t^2 - s^2 = (t + s)(t - s)$.

The equation gives the 1 to 1 correspondence between the two ways of writing n .

If $n = ab$ with a and b close together, then $s = a - b/2$ is small and so t is slightly larger than \sqrt{n} . So we find a and b by trying all values for t starting with $[\sqrt{n}] + 1$ until we find $t^2 - n = s^2$ is a perfect square.

Example : Factor 200819

Solution : We have $\sqrt{200819} + 1 = 449$. Now $449^2 - 200819 = 782$ which is not a perfect square. Next we try

$$t = 450 . 450^2 - 200819 = 1681 = 41^2.$$

Then $200819 = 450^2 - 41^2 = (450 + 41)(450 - 41) = 491.409$.

For finding a and b we try to find

$$t = [\sqrt{n}] + 1, [\sqrt{n}] + 2 \dots$$

Also we choose a small k , successively set $t = [\sqrt{kn}] + 1, [\sqrt{kn}] + 2, \dots$ until we obtain a t for which $t^2 - kn = s^2$ is a perfect square.

Exercise : Factor 141467.

SOME COMPUTER PROGRAM FOR FINDING PRIME FACTORS OF ANY INTEGER.

The following BASIC program will find the prime factors of any integer. The integer is input to the program as data. the program terminates execution whenever a zero is typed as input.

```

100      REM PRIME FACTORS OF ANY INTEGER
110      PRINT "PRIME FACTORS OF ANY INTEGER"
120      PRINT
130      PRINT
140      PRINT
150      PRINT "NUMBER TO BE FACTORED IS";
160      INPUT A
170      IF ABS (A) <= 1 THEN 340
180      LET N = INT (ABS(A))
190      REM FIND AND PRINT PRIMES
200      LET B = 0
210      FOR I = 2 TO N/2

```

```

220   IF N/I > INT (N/I) THEN 300
230   LET B = B + 1
240   IF B > 1 THEN 260
250   PRINT "PRIME FACTORS OF "; N; "ARE"
260   PRINT 1 ;
270   LET N = N/I
280   IF N = 1 THEN 120
290   LET I = I - 1
300   NEXT I
310   IF N <> INT (A) THEN 120
320   PRINT N; " IS A PRIME NUMBER"
330   GOTO 130
340   END

```

RUN

PRIME FACTORS OF ANY INTEGER

NUMBER TO BE FACTORED IS ? 56

PRIME FACTORS 56 ARE

2 2 2 7

NUMBER TO BE FACTORED IS ? 346

PRIME FACTORS OF 346 ARE

2 173

NUMBER TO BE FACORED IS ? 397

397 IS A PRIME NUMBER

NUMBER TO BE FACTORED IS ? 560

PRIME FACTORS OF 560 ARE

2 2 2 2 5 7

The following BASIC program uses Fermat's method to compute the largest factor of a given integer.

```

100   REM LARGEST FACTOR OF ANY NUMBER
110   PRINT "WHAT IS THE NUMBER";
120   INPUT N
130   IF N = 0 THEN 280
140   LET W = INT (SQR (N))

```

```
150      LET X = 2 * W+1
160      LET Y = 1
170      LET R= W* W-N
180      IF R = 0 THEN 250
190      IF R> 0 THEN 220
200      LET R = R +X
210      LET X = X+2
220      LET R = R-Y
230      LET Y = Y+ 2
240      GOTO 180
250      LET F = (X-Y)/2
260      PRINT "LARGEST FACTOR OF “; N;”IS”; F
270      GOTO 110
280      END
```

RUN

```
WHAT IS THE NUMBER? 311
LARGEST FACTOR OF 311 IS 1
WHAT IS THE NUMBER ? 45
LARGEST FACTOR OF 45 IS 5
WAT IS THE NUMBER ? 0
```

The BASIC program shown below computes the largest factor of the number listed in DATA statement.

```
100      REM LARGEST FACTOR PROGRAM
110      READ N
120      FOR D = 2 TO SQR (N)
130      IF N/D = INT (N/D) THEN 170
140      NEXT D
150      PRINT N, "IS A PRIME NUMBER"
160      GOTO 110
170      PRINT N/D, "IS THE LARGEST FACTOR OF “;N
180      GOTO 110
```

```

190 DATA 3394, 5799, 2827, 1907, 9115
200 DATA 2807, 1495, 373, 19, 206
210 END

```

RUN

```

1697 IS THE LARGEST FACTOR OF 3394
1933 IS THE LARGEST FACTOR OF 5799
257 IS THE LARGEST FACTOR OF 2827
1907 IS A PRIME NUMBER
1823 IS THE LARGEST FACTOR OF 9115
401 IS THE LARGEST FACTOR OF 2807
299 IS THE LARGEST FACTOR OF 1495
373 IS A PRIME NUMBER
19 IS A PRIME NUMBER
103 IS THE LARGEST FACTOR OF 206

```

OUT OF DATA IN LINE 110

To find all pairs of factors of an integer, use the following BASIC program.

```

100 REM PAIRS OF FACTORS OF AN INTEGER
110 PRINT "PAIRS OF FACTORS"
120 PRINT
130 PRINT
140 PRINT "TYPE THE INTEGER";
150 INPUT X
160 PRINT
170 PRINT "THE PAIRS OF FACTORS OF ";X;"ARE:"
180 FOR A = 1 TO SQR (ABS (X))
190 IF INT (X/A) <> X/A THEN 210
200 PRINT A, X/A
210 NEXT A
220 PRINT
230 PRINT

```

```

240      PRINT "TYPE 1 TO STOP; 2 TO CONTINUE";
250      INPUT T
260      IF T <> 1 THEN 120
270      END

```

RUN

PAIRS OF FACTORS

TYPE THE INTEGER? 8960

THE PAIRS OF FACTORS OF 8960 ARE :

1	8960
2	4480
4	2240
5	1792
7	1280
8	1120
10	896
14	640
16	560
20	448
28	320
32	280
35	256
40	224
56	160
64	140
70	128
80	112

TYPE 1 TO STOP ; 2 TO CONTINUE?2

TYPE THE INTEGER ? 4680

THE PAIRS OF FACTORS OF 4680 ARE :

1	4680
2	2340
3	1560
4	1170
5	936
6	780
8	585
9	520
10	468
12	390
13	360
15	312
18	260
20	234
24	195
26	180
30	156
36	130
39	120
40	117
45	104
52	90
60	78
65	72

TYPE 1 TO STOP; 2 TO CONTINUE ? 1

EXERCISE

1. Find all bases for which 21 is a pseudoprime.
2. Prove that no integer of the form $n = 3p$ (with $p > 3$ prime) can be pseudoprime to the base 2, 5 or 7.
3. prove that 91 is the smallest pseudoprime to the base 3.
4. Prove that 341 is the smallest pseudoprime to the base 2.
5. Let $n = pq$ be a product of two distinct primes. Let $d = \gcd(p-1, q-1)$ prove that n is a pseudoprime to the base b if and only of $b^d \equiv 1 \pmod{n}$.

6. Prove that there are infinitely many pseudoprime to the base b for $b = 2, 3, 5$.
7. Show by pseudoprime primality test that $2047 = 2^{11} - 1$ is composite.
8. Show that the following are Carmichael numbers,
6601, 29341, 172081, 2465.
9. Show that 65 is a strong pseudoprime to the base 8 and to the base 18, but not to the base 14.
10. Factor $n = 8051$ using rho method with $f(x) = x^2 + 1$, $x_0 = 1$.
11. Factor 2701 with $f(x) = x^3 = x + 1$, $x_0 = 1$.
12. Use Fermat factorization to factor : (a) 809009 (b) 8633 (d) 4601.
13. Prove that all Carmichael numbers are odd.
14. Verify that 2047 is the smallest strong pseudoprime to the base 2.
15. Show that 2047 is a composite number using strong pseudoprime primality test.



ANSWER TO EXERCISES

CHAPTER II.

1. (i) 2592 (ii) 22400 (iii) 1800 (iv) 320204 (v) 312 (vi) 720
(viii) 1152

CHAPTER III.

1. 4 and 6
5. 7
6. 143
7. 89
8. (a) No solution
(b) $x = 45,94 \pmod{98}$
(c) $x \equiv 16, 59, 102, 145, 188, 231 \text{ and } 274 \pmod{301}$
(d) $x = 6, 13 \text{ and } 20 \pmod{21}$
9. (a) $x \equiv 4944 \pmod{9889}$ (b) $x \equiv 785 \pmod{1122}$ (c) $x \equiv 52 \pmod{105}$
11. 13
16. $x \equiv 3, 4, 10, 39 \pmod{7}$ are only solutions of the congruence
19. 15
24. $3^2 \cdot 7 \cdot 13 \cdot 7^2$
25. 82, 43
26. 23

CHAPTER IV. NIL

CHAPTER V. NIL

CHAPTER VI.

1. $\text{ind}_2 5 = 9, \text{ind}_6 5 = 9, \text{ind}_7 5 = 3, \text{ind}_{11} 5 = 3.$
2. 14
4. $x \equiv 7, 8 \text{ and } 11 \pmod{13}.$
5. (i) $x = 7 + 11t, t = \pm 1, \pm 2, \dots$
 (ii) $x = 22 + 23t, t = 0, \pm 1, \pm 2, \dots$
 (iii) $x = 7, 29, 57, \dots, -15, -37.$
6. Solvable.
7. $b \equiv 1, 3, 9 \pmod{13}$
8. (a) $x \equiv 7 \pmod{11}$
 (b) $x \equiv 5, 6 \pmod{11}$
 (c) No solution .
10. None

CHAPTER VII.

- 2 (i) -1 , (ii) -1 , (iii) -1 (iv) 1 (v) $+1$ (vi) $+1.$
5. $x \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$
8. (a) solvable (b) Not solvable (c) solvable 10. (a) -1 , (b) -1 ,
 (c) 1

CHAPTER VIII.

1. 8, 13
10. 83, 97
11. 37. 73
12. (a) 823. 983
 (b) 89.97
 (c) 43.107.



APPENDIX

THE CHRONOLOGY OF PRIME NUMBER RECORDS

The Largest Known Prime Records.

On January 27, 1998, the team of Roland Clarkson, George Woltman, Scott Kurowskii et al discovered a new prime record: $2^{3021377} - 1$. In June 1999 largest known prime $2^{6972593} - 1$ having 2,098,960 digits in found by Nayan Hajratwala.

Date	Prime	Digits	Who
Jan 1998	$2^{3021377} - 1$	909526	Clarkson, Woltman, Kurowski, et al. (GIMPS)
Aug 1997	$2^{2976221} - 1$	895932	Spence, Woltman, et al. (GIMPS)
Nov 1996	$2^{1398269} - 1$	420921	Armengaud, Woltman, et al (GIMPS)
Sep 1996	$2^{1257787} - 1$	378632	Slowinski and Gage
Jan 1994	$2^{859433} - 1$	258716	Slowinski and Gage
Feb 1992	$2^{756839} - 1$	227832	Slowinski and Gage
Aug 1989	$391581 \cdot 2^{216193} - 1$	65087	Brown, Noll, Parady, Smith G, Smith J and Zarantonello
Sep 1985	$2^{216091} - 1$	65050	Slowinski
1983	$2^{132049} - 1$	39751	Slowinski
1982	$2^{86243} - 1$	25962	Slowinski
1979	$2^{44497} - 1$	13395	Nelson and Slowinski

Feb 1979	$2^{23209} - 1$	6987	Noll
Oct 1978	$2^{21701} - 1$	6533	Nickel and Noll
1971	$2^{19937} - 1$	6002	Tuckerman
1963	$2^{11213} - 1$	3376	Gillies
1961	$2^{4423} - 1$	1332	Hurwitz
1957	$2^{3217} - 1$	969	Riesel
1952	$2^{2281} - 1$	687	Robinson
Jan 1952	$2^{607} - 1$	183	Robinson
Jul 1951	$180 \cdot (2^{127} - 1)^2 + 1$	79	Miller and Wheeler
1951	$(2^{148} + 1)/17$	44	Ferrier
1876	$2^{127} - 1$	39	Lucas
1867	$(2^{53} + 1)/(3 \cdot 107)$	14	Landry
1851	999999000001	12	Looff
1771	$2^{31} - 1$	10	Euler

THE TWIN PRIME RECORDS

On August 31, 1998, Ray Ballinger has found a 11751 digits twin primes record with "Proth" written by Yves Gallot: $835335 \cdot 2^{39014} \pm 1$.

Date	Prime	Digits	Who
Aug 1998	$835335 \cdot 2^{39014} \pm 1$	11751	Ballinger and Gallot
Nov 1995	$242206083 \cdot 2^{38880} \pm 1$	11713	Indlekofer and Jarai
Oct 1995	$570918348 \cdot 2^{5120} \pm 1$	5129	Dubner
Nov 1994	$697053813 \cdot 2^{16352} \pm 1$	4932	Indlekofer and Jarai
1993	$4655478828 \cdot 10^{5120} \pm 1$	3439	Dubner
1989	$1706595 \cdot 2^{11235} \pm 1$	3389	Brown, Noll, Parady, Smith G, Smith J and Zarantonello

THE MERSENNE PRIME RECORDS

Mersens primes are of the form $2^p - 1$.

On January 27, 1998, the team of Roland Clarkson, George Woltman, Scott Kurowskii et al discovered a new prime record: $2^{3021377} - 1$.

Date	Prime	Digits	Who
Jan 1998	$2^{3021377} - 1$	909526	Clarkson, Woltman, Kurowski, et al. (GIMPS)
Aug 1997	$2^{2976221} - 1$	895932	Spence, Woltman, et al. (GIMPS)
Nov 1996	$2^{1398269} - 1$	420921	Armengaud, Woltman, et al (GIMPS)
Sep 1996	$2^{1257787} - 1$	378632	Slowinski and Gage
Jan 1994	$2^{859433} - 1$	258716	Slowinski and Gage
Feb 1992	$2^{756839} - 1$	227832	Slowinski and Gage
Aug 1989	$391581 \cdot 2^{216193} - 1$	65087	Brown, Noll, Parady, Smith G, Smith J and Zarantonello
Sep 1985	$2^{216091} - 1$	65050	Slowinski
1983	$2^{132049} - 1$	39751	Slowinski
1982	$2^{86243} - 1$	25962	Slowinski
1979	$2^{44497} - 1$	13395	Nelson and Slowinski
Feb 1979	$2^{23209} - 1$	6987	Noll
Oct 1978	$2^{21701} - 1$	6533	Nickel and Noll
1971	$2^{19937} - 1$	6002	Tuckerman
1963	$2^{11213} - 1$	3376	Gillies
1961	$2^{4423} - 1$	1332	Hurwitz
1957	$2^{3217} - 1$	969	Riesel
1952	$2^{2281} - 1$	687	Robinson
Jan 1952	$2^{607} - 1$	183	Robinson
1876	$2^{127} - 1$	39	Lucas
771	$2^{31} - 1$	10	Euler

The 38th Mersenne prime is $2^{6972593} - 1$ is found in June 1998

Number of the form $n! \pm 1$ are called factorial primes.

Date	Prime	Digits	Who
1998	$6917! - 1$	23560	Caldwell and Gallot
1993	$3610! - 1$	11277	Caldwell
1992	$3507! - 1$	10912	Caldwell
1992	$1963! - 1$	5614	Caldwell and Dubner
1984	$1477! - 1$	4042	Dubner
1983	$872! - 1$	2188	Dubner
1981	$469! - 1$	1051	Buhler, Crandall and Penk

Primorial Primes are of the form $2.3.5 \dots p+1$.

Date	Prime	Digits	Who
1993	$24029\# + 1$	10387	Caldwell
1989	$18523\# + 1$	8002	Dubner
1987	$13649\# + 1$	5862	Dubner
1986	$11549\# + 1$	4951	Dubner
1984	$4787\# + 1$	2038	Dubner
1982	$2657\# + 1$	1115	Buhler, Crandall and Penk



BIBLIOGRAPHY

1. Andrews; G. E. : Number Theory, Hindustan Publishing Corporation, Delhi 1992.
2. Apostol, Tom. M. : An Intoduction to Analytic Number Theory, Springer Verlag, Narosa, 1977.
3. Barnett, I. A. : Elements of Number Theory, Prindle, Weber and Schmidt Inc. 1969.
4. Burton, David M. : Elementary Number Theory, Universal Book Stall, New Delhi, 1994.
5. Gelfond and Linnik : Elementary Methods in Analytic Number Theory, Rand N C Nally and Company, Chicago, 1965.
6. Griffith Harriet : Elementary Theory of Numbers Mc. Graw Hill Book Co. Inc. 1954.
7. Hardy, G. H. and Wright, E. M., An Introduction to Theory of Numbers, Oxford, Clarendon Press, 1960.
8. Kirch, Allan M. : Elementary Number Theory, A Computer Approach. Index Educational Publishers, New York.
9. Koblintz, N. : A Course in Number Theory and Cryptogarphy, Springer Verlag, 1982.
10. Kumanduri, Ramanujachari and Romeo Cristina : Number Theory with Computer Applications, Prentice Hall, India, New Delhi, 1985.
11. Landau, Edmund : Elementary Number Theory, Chelsea Publication Company, 1966.
12. Leveque, William J. : Fundamentals of Number Theory : Addison-Wisely Publication Company, 1977.
13. Leveque, William J. : Reviews in Number Theory, American Mathematical Society, 1974.
14. Nagell, Trygve : Introduction to Number Theory, Chelsea Publishing Company, New York, 1964.

15. Ribenboim Paulo : *The Book of Prime Number Records*. Springer Verlag, 1988.
16. Ribenboim Paulo : *The Little Book of Big Primes*, Springer Verlag, 1991.
17. Schroeder, Manfred : *Number Theory in Science and Communication*, 2nd Edition, Springer Verlag, 1987.
18. Shanks, Daniel : *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1985.
19. Sierpinski, Waclaw : *Elementary Theory of Numbers*: Transaction Hulanicki Warsaw, 1964.
20. Spencer, Donald D : *Computers in Number Theory*, Computer Science Press, USA, 1982.
21. Spencer, Donald D : *Exploring Number Theory in Microcomputers*, Camelot Publishing Company, Florida 1991.
22. Telang, S. G. : *Number Theory*, Tata McGraw Hill Publishing Company Ltd., New Delhi, 1996.



INDEX

- Abel, Niels Henrick, 108
Abel's identity, 108
Abundant number, 37, 38
Affine map, 127
Affine Transformation, 127
Algorithm, 7, 87, 184
Amicable number, 33, 35, 47
Andrews, G.E., 203
Apostol, Tom M., 203
Arithmetic, Fundamental theorem of, 6
Arithmetical functions, $d(n)$ & $\sigma(n)$, 48, 59
Armengaud, 198, 201
Armstrong number, 35
Average of an arithmetical function, 64
Ballinger and Gallot, 200
Barnett, I. A., 203
Bertrand postulate, 10
Brent, P., 16
Brun : 16
Brown, Noll, 198
Buhler, Crandall and Penk, 202
Burton, David M., 203
Caesar, Julius, 125
Caesar cipher, 125, 126
Caldwell, 202
Caldwell and Dubner, 202
Caldwell and Gallot, 202
Cancellation law, 80, 91
Carmichael number, 180, 181, 182, 195
Chebyshev function $\vartheta(x)$, 106, 107
Chebyshev function $\psi(x)$, 106, 107
Chebyshev, Pafnuti Liwovich, 106
Chinese Remainder Theorem, 98, 100, 102, 181
Cipher, 125, 126
Ciphertext, 124, 125, 126, 127, 129
Clarkson, 198, 201
Classical cryptosystem, 124, 125, 130
Complete Residue system, 80, 81, 90
Completely multiplicative function, 50
Congruence, 75
Crandall and Buhler, 202
Cryptography, 124, 132, 174, 178, 185, 186
Deciphering transformation, 124
Deficient number, 37, 38
Digraph, 124, 128

- Dirichlet, 69
- Discrete log method, 133
- Discrete logarithm, 149, 188
- Disquisitiones Arithmeticae, 75
- Distribution of prime numbers, 31
- Division algorithm, 7
- Divisor function, 49, 59
- Dubner, 200, 202
- Dubner and Caldwell, 202
- EIGamal, T., 133
- EIGamal cryptosystem, 185, 186
- Eratosthenese, 1, 36
- Euclid, 10
- Euclid's lemma, 5
- Euclidean algorithm, 7, 9
- Euler, Leonhard, 18
- Euler Fermat theorem, 82, 83, 86, 92, 135
- Euler Function, 50
- Euler Pseudoprime, 179, 180
- Euler's criterion, 155, 156, 157
- Euler's summation formula, 62
- Euler totient function, $\phi(n)$, 50
- Exponential modulo m , 87
- Fermat number, 19, 24, 44, 45
- Fermat Primes, 19, 24
- Fermat, Pierre de, 19, 24
- Fermat's factorization theorem, 188, 195
- Fermat's theorem, 81, 82, 84, 85
- Ferrier, 199
- Fibonacci number 43, 44, 45
- Friendly number, 33, 35
- Fundamental Theorem of Arithmetic, 6
- Gage, 198
- Gallot and Caldwell, 202
- Gauss, Carl Friedrich, 106, 153
- Gauss Lemma, 158
- Gelfond and Linnik, 203
- Generalised Euler function, 61
- Gillies, 199
- GIMPS, 198
- Goldbach, C., 17
- Goldbach conjecture, 17
- Greatest Common Divisor, 4
- Greatest integer function, 53, 109
- Griffith, H., 203
- Hardy, Godfrey Harold, 19, 203
- Hurwitz, 199
- Identification schemes, 174
- Identity Function $I(n)$, 49
- Indlekofer and Jarai, 200
- Indices, 134, 146, 147, 148
- Inversion formula, Mobius, 120
- Jacobi, Carl Gustav Jacob, 166
- Jacobi symbol, 166, 177, 183
- Jarai and Indlekofer, 200
- Keller, 20
- Kirch, Allan M., 203
- Knapsack problem, 133
- Koblitz, N., 203
- Kumanduri Ramanujan, 203
- Kurowski, 198, 201
- Landau, Edmund, 203
- Landry, 199

- Langrange, Joseph Louis, 93, 94
 Langrange's theorem on polynomial congruences, 93, 94, 95, 151
 Lattice point, 68, 69
 Law of quadratic reciprocity, 161, 169
 Least common multiple (lcm), 140
 Legendre Adrein-Marie, 116
 Legendre, 106, 155
 Legendre's identits, 116
 Legendre's symbol, 155, 156, 166, 177
 Lehemer, Derrick Henry, 185
 Leveque, W.J., 203
 Linear congruence, 89, 90, 91, 92
 Linnik and Gelfond, 203
 Liouville, Joseph, 62
 Little Fermat Theorem, 81, 82, 84
 Littlewood, John Edensor, 19
 Livoville's function $\lambda(n)$, 62
 Loeff, 199
 Lucas, Edouard, 185, 199
 Lucas-Lehmer, 185
 Lucas-Lehmer Primality test, 185
 Lucky number, 36
 M. Makowski, 18
 Magic square, 30, 31
 Mangoldt function $\Lambda(n)$, 63
 Massey-Omura cryptosystem, 133
 Mersenne, P., 25
 Mersenne number, 25, 28, 46, 183
 Mersenne Prime, 25
 Miller and Wheeler, 199
 Mobius function $\mu(n)$, 48, 49, 119
 Multiplication function, 50, 61, 62
 Nagell, T., 203
 Nayan Hajratwala, 13, 28
 Nelson and slowinski, 198
 Nickel and Noll, 198
 Noll, 198
 Non-residue, 153
 Number Theoretic Function, 48
 O' big oh notation, 64
 Paraday, 200
 Perfect number, 26, 27, 37, 47, 74, 101
 Personal Identification Number (PIN), 174
 Plaintext, 124, 126
 Pollard's p-1 method, 187
 Pollard's rho-method, 188
 Polynomial congruence, 93
 Primality testing, 134, 178, 182, 184
 Prime, 1, 29
 Prime factorization Tau (N), Sigma (N), 70
 Prime number, 1, 30, 38, 39, 40, 44, 45
 Prime number Theorem, 32, 106, 107, 108, 119, 120
 Primitive modulo prime, 141
 Primitive root, 134, 136, 139, 185
 Primitive root modulo p^k , 142
 Primitive root modulo $2p^k$, 144
 Probabilistic Primality Testing, 182, 183, 184, 185
 Probable prime, 184
 Pseudoprime, 178, 184, 195

- Public Key Cryptography, 128, 129, 130, 186
 Public key cryptosystem, 129
 Quadratic congruences, 90, 96
 Quadratic non-residue, 153, 164
 Quadratic Reciprocity Law, 161
 Quadratic Residue, 151, 153, 164
 Rabin-Miller Probabilistic Primality Test, 185
 Ramanujan, Srinivasa, 30
 Reciprocity Law, 161
 Reduced Residue system, 81, 82, 139
 Relatively Prime, 56
 Repunit, 17
 Residue classes, 80
 Residue, quadratic, 151, 153, 164
 Residue system, complete, 80, 81
 Residue system, reduced, 81, 82, 139
 Ribenboim, Paulo, 204
 Riesel, 199
 Robinson, Raphael M., 12, 26
 RSA cryptosystem, 131
 Satyanarayanan, M., 30
 Schinzel, 17
 Schroeder, Manfred, 204
 Shamir, 131
 Shanks, Daniel, 204
 Shift transformation, 126
 Sieve, 1, 36
 Sierpinski, Wacław, 204
 Sigma (N) 70, 71, 72, 73
 Simple Primality Test, 178
 Simultaneous Linear Congruence, 98
 Slowinski, 198
 Smith, G., 200
 Smith, J., 200
 Spence, 198, 201
 Spencer, D.D., 204
 Square root modulo p , 170, 172
 Strong pseudoprime, 182, 183, 184, 185, 195
 Summation formula of Euler, 65
 Summatory Function, 50
 Symbol, Jacobi, 166
 Tau (N), 70, 71, 72, 73
 Telang, S.G., 204
 Titanic prime, 12
 Totient function $\phi(n)$, 48
 Triangular number, 29, 46
 Trigraph, 124, 128
 Tuckerman, 199
 Twin prime conjecture, 15
 Twin prime, 13, 14
 Ulam, S. M., 36
 Vinogradov, I.M., 18
 Von Mangoldt, H., 63
 Von-Mangoldt function, $\Lambda(n)$ 63
 Wilson, John, 95
 Wilson's Theorem, 95, 96, 97, 98
 Woltman, 198, 201
 Wright, E.M., 203
 Zarantonell, 200

